

Universidade do Minho
Escola de Engenharia

Pedro José Gonçalves Oliveira

New Approaches to risk management in It projects with high uncertainty

May of 2025

New Approaches to risk management in IT projects with high uncertainty
Pedro José Gonçalves Oliveira
UMinho | 2025



Universidade do Minho
Escola de Engenharia

Pedro José Gonçalves Oliveira

New Approaches to risk management in IT projects with high uncertainty

Master's Work Project[Dissertation] Report
Integrated Master's in Engineering and Management of Information Systems

Work performed under the supervision of
Professor Pedro Miguel Gonzalez Abreu Ribeiro
Jan Valdman

May of 2025

COPYRIGHT AND TERMS OF USE OF THE WORK BY THIRD PARTIES

This is an academic work that can be used by third parties as long as the internationally accepted rules and good practices are respected, with regard to copyright and related rights.

Thus, the present work can be used under the terms foreseen in the license indicated below.

If the user needs permission to be able to use the work under conditions not provided for in the indicated licensing, he/she should contact the author, through the RepositóriUM of the University of Minho.

Licença concedida aos utilizadores deste trabalho

[Caso o autor pretenda usar uma das licenças Creative Commons, deve escolher e deixar apenas um dos seguintes ícones e respetivo lettering e URL, eliminando o texto em itálico que se lhe segue. Contudo, é possível optar por outro tipo de licença, devendo, nesse caso, ser incluída a informação necessária adaptando devidamente esta minuta]



Atribuição
CC BY
https://creativecommons.org/licenses/by/4.0/
[Esta licença permite que outros distribuam, remixem, adaptem e criem a partir do seu trabalho, mesmo para fins comerciais, desde que lhe atribuam o devido crédito pela criação original. É a licença mais flexível de todas as licenças disponíveis. É recomendada para maximizar a disseminação e uso dos materiais licenciados.]

ACKNOWLEDGMENTS

After five years of study and work, and upon completing my dissertation, I owe my sincere thanks to all those who took part in this journey. To Professor Pedro Ribeiro, for his availability, knowledge sharing, promptness, guidance, and support throughout this stage and during times of difficulty and to Professor Jan Valdman for his availability, support and for showing me different ways of approaching problems. To my sister and my parents, for their encouragement and constant motivation at the right moments. To my friends, for their unwavering companionship, for always believing in me, and encouraging me to give my best. No journey is made alone, and therefore, my eternal gratitude and recognition go to all those who, in some way, took part in this stage

STATEMENT OF INTEGRITY

I hereby declare having conducted this academic work with integrity. I confirm that I have not used plagiarism or any form of undue use of information or falsification of results along the process leading to its elaboration.

I further declare that I have fully acknowledged the Code of Ethical Conduct of the University of Minho.

ABSTRACT

Risk management has become an increasingly critical component of successful IT project execution, particularly in environments marked by high levels of uncertainty. Traditional risk management models, while widely used, often lack the flexibility and predictive capabilities needed to address the challenges of complex, dynamic IT projects.

Recognizing this gap, the present study proposes the development of an integrated risk management framework that combines the structural strengths of internationally recognized standards—namely ISO 31000 and COSO ERM—with innovative, technology-driven approaches such as Artificial Intelligence (AI), Digital Twins, and Behavioural Science. These tools are intended to provide real-time insights, enhance foresight, and support proactive decision-making.

To support the creation and validation of this framework, a detailed analysis of existing standards and methodologies was conducted, along with a review of future trends in the risk management field. The research follows a Design Science Research approach to iteratively design, refine, and evaluate the proposed framework.

The outcome is a model that offers greater adaptability, improved collaboration across organizational levels, and enhanced cost efficiency in resource allocation. A validation process was conducted to assess its effectiveness, with findings confirming its practical value while also identifying areas—such as scalability and implementation guidance—that require further refinement.

This work contributes to the ongoing evolution of project risk management by offering a robust and forward-looking tool that organizations can adapt to better navigate risk in uncertain and complex IT project environments.

1. TABLE OF CONTENTS

Copyright and Terms of Use of the Work by Third Parties v

Acknowledgments vi

Statement of Integrity vii

Abstract viii

List of Abbreviations and Acronyms xi

List of Figures xii

List of Tables xii

1.Introduction 1

1.1 Context 1

1.2 Objectives and expected results. 2

1.3 Methodological approach 2

1.4 Document structure 4

2. Literature Review 6

2.1 Risk 6

2.1.1 What is Risk? 6

2.1.2 Types of Risks 8

2.1.3 What Causes Risks? 10

2.1.4 The definition of Project Risk Management 12

2.1.5 Risk Management Strategies 14

2.2 The Concept of Uncertainty in IT projects 16

2.2.1 Impact on risk management 17

2.3 Main Frameworks 18

2.3.1 ISO 31000 18

2.3.2 COSO ERM 22

2.4 Future Trends 25
3. Risk Management Process Frameworks 31
3.1 Risk Management in ISO 31000-2018 31
3.1.1 Processes in ISO 31000-2018 32
3.1.2 Challenges 45
3.2 Risk Management in COSO ERM 2017 46
3.2.1 Processes in COSO ERM 2017 47
3.2.2 Challenges 51
3.3 Comparison between COSO ERM and ISO 31000 52
3.4 COSO ERM and ISO 31000:1v1 during the process 54
4. New Approaches to Risk Management 59
4.1 Digital Twins applied to Risk Management 59
4.2 Artificial intelligence and Machine Learning applied to Risk Management 63
4.3 Application of Behavioural Science in Risk Management 67
5. iRISK(Intelligent Risk Integration and Strategic Knowledge)Framework 71
5.1 The base of the iRISK Framework 71
5.2 New approaches into the iRISK framework 74
5.3 Integration and Implementation Strategy 76
5.4 Benefits of the iRISK Framework 78
6. Validation 81
6.1 Evaluation Methodology 81
6.2 Results of Validation 82
Strengths of the Framework 82
Areas for Improvement 82
6.3 Comparative Evaluation 83

6.4 Key Validation Findings 83
6.5 Final Evaluation and Future Perspectives 84
7. Conclusion 85
7.1 Summary of Findings 85
7.2 Contributions to Knowledge 85
7.3 Practical Implications 86
7.4 Limitations and Future Research 86
7.5 Final Remarks 87
References 88
Appendix 92

LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation	Full Term
AI	Artificial Intelligence
APM	Association for Project Management
COSO	Committee of Sponsoring Organizations of the Treadway Commission
ERM	Enterprise Risk Management
IS	Information System
IT	Information Technology
ML	Machine Learning
PM	Project Management
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
RFID	Radio-Frequency Identification

LIST OF FIGURES

Figure 1- The relationship between the stages of the risk management 16
Figure 2-The ISO 31000 guideline 21
Figure 3-COSO ERM Framework 23
Figure 4- Digital Twin components and high-level processes. 30
Figure 5-ISO 31000-2018 Process 31
Figure 6- Risk Controls 40
Figure 7-Process in COSO ERM 2017 47
Figure 8-Traditional (Left) vs. Digital Twin-Driven Risk Management (Right) 62
Figure 9-AI integrated in ISO 31000 2018 Process 67
Figure 10-COSO and ISO integrated in detail 74
Figure 11-iRISK Framework simplified 76
Figure 12-iRISK Framework 80

LIST OF TABLES

Table 1-Comparison between COSO ERM and ISO 31000 54
Table 2-ISO 31000 Summary 54
Table 3-COSO ERM 2017 55
Table 4-Implementation Strategy 78
Table 5-Comparative Evaluation 83

1. INTRODUCTION

1.1 Context

In the dynamic landscape of Information Technology (IT) projects, where uncertainty looms large, the need for innovative and adaptive risk management approaches has never been more critical. As organizations increasingly embark on complex IT initiatives with multifaceted dependencies, the traditional methodologies often fall short in addressing the intricacies of high uncertainty environments. This Master's thesis seeks to explore and propose new approaches to risk management tailored specifically for IT project environments characterized by elevated uncertainty levels.

The accelerating pace of technological evolution, coupled with the complex interplay of factors such as market dynamics, regulatory changes, and emerging technologies, underscores the complexity of risk within IT projects. Traditional risk management practices, while effective in stable environments, face challenges in providing adequate foresight and mitigation strategies in the face of pervasive uncertainty.

This research seeks to explore the existing gaps and limitations in current risk management paradigms for IT projects operating under high uncertainty. By exploring the shortcomings of established methodologies, the aim is to identify novel strategies and frameworks that can dynamically adapt to the evolving risk landscape inherent in IT endeavours.

The research will include a comprehensive review of existing literature, case studies, and real-world examples to distil key insights into the unique challenges posed by uncertainty in IT project environments. Building on this foundation, the thesis seeks to propose innovative risk management approaches that not only recognise the unpredictable nature of IT projects but also capitalize on uncertainty as a potential source of opportunity.

Through a blend of theoretical frameworks and practical applications, this research aims to contribute to the advancement of risk management practices in IT projects. By providing nuanced insights and proposing adaptive methodologies, the thesis endeavours to empower organizations to navigate the uncertainties inherent in the IT landscape with resilience and strategic acumen.

As we enter a digital era characterised by innovation and disruption, the importance of pioneering risk management approaches tailored to high uncertainty IT environments is becoming a critical facet in ensuring the success and sustainability of IT projects. This thesis aims to be a beacon in this endeavour

by identifying new ways for organizations to proactively embrace and leverage uncertainty in the pursuit of successful IT project outcomes.

1.2 Objectives and expected results.

This thesis aims to contribute to the field of risk management in Information Technology (IT) projects by addressing the challenges posed by high uncertainty. The objectives include a comprehensive review of current practices in IT project risk management, an assessment of specific factors contributing to uncertainty, an exploration of emerging techniques, the development of an innovative risk management framework, and an assessment of implementation challenges. By carrying out a correct, thorough and careful analysis of the premises, the aim is to achieve a set of results that will be fundamental to the development of this dissertation, namely:

- Characterization of current IT project environments.
- Systematization of new strategies / approaches to risk management in IT projects
- Study of future trends in risk management.
- Development of an initial framework with synthesis and guidelines for risk management in IT projects.

The pursuit of these objectives will lead to a better understanding of the impact of risk management on the achievement of the intended outcome in a project, thus contributing to a more informed and conscious approach to risk management in a project.

1.3 Methodological approach

This dissertation focuses on new approaches to risk management in highly uncertain IT project environments, using the methodological approach of DSR (Design Science Research).

Design Science Research (DSR) is a research paradigm that focuses on the creation and evaluation of innovative artifacts to solve real-world problems(Hevner et al. 2004). When applied to this dissertation thesis on new approaches to risk management in highly uncertain IT project environments, DSR can provide a structured framework for the development and validation of novel solutions. This methodological approach is characterized by its focus on creating and evaluating artifacts that address specific problems. In the context of IT project risk management, these artifacts could be new methods, frameworks, or tools designed to improve risk management practices in uncertain environments (Venable, Pries-Heje, and Baskerville 2016).

The alignment of DSR with the research plan is reflected in the three iterative cycles:

- Relevance Cycle:

  This cycle connects the research to the real-world context by identifying the limitations of existing models (ISO 31000, COSO ERM) in managing risks in highly uncertain IT projects. These limitations informed the requirements for a new approach that would integrate adaptive, data-driven, and behavioural science elements.

- Design Cycle:

  The iRISK Framework was developed iteratively in this phase. The framework integrates three modules:

  1. A Data-Driven Monitoring Layer to provide real-time insights.
  2. A Cognitive Intelligence Module to incorporate advanced analytics and AI-driven decision support.
  3. A Behavioural Engagement Toolkit to foster a risk-aware culture and address cognitive biases in risk perception.

     Each module was designed, evaluated, and refined through an iterative process supported by literature and expert input.

- Rigor Cycle:

  The framework builds upon established theoretical foundations and was validated through structured interviews with three domain experts. Their feedback confirmed the framework's conceptual relevance and practical applicability while also highlighting areas for improvement, such as scalability and contextualization across diverse organizational settings.

Key Artifacts Created in this Research:

- The conceptual iRISK Framework.
- A detailed description of its modular architecture.
- Validation reports and expert feedback analysis.

This structured application of DSR allowed for the rigorous development and evaluation of iRISK, ensuring it addresses both academic and practical dimensions of IT project risk management.

In summary, applying DSR to this dissertation on new approaches to risk management in uncertain IT project environments provides a structured, rigorous methodology for developing and validating innovative solutions. By following the DSR framework, using evaluation strategies such as FEDS, and

addressing limitations, this dissertation can make a significant contribution to both the theoretical understanding and practical application of risk management in challenging IT project contexts.

1.4 Document structure

The structure of this dissertation is carefully organized to support the development of new approaches to risk management in IT projects under conditions of high uncertainty. Each chapter builds on the last, offering a logical and cohesive narrative that guides the reader from the research context to the final conclusions and future recommendations.

The opening chapter introduces the study by contextualizing the challenges faced in IT project environments where uncertainty is a critical factor. It outlines the motivation behind the research, the specific objectives pursued, and the methodological approach employed—namely, Design Science Research. This introductory section also presents the overall structure of the dissertation, establishing a roadmap for the chapters that follow.

The second chapter is dedicated to the literature review and explores the conceptual foundation necessary for understanding the study's core themes. It begins by examining the definitions of risk and uncertainty, their causes, and types. It then transitions into a discussion of established risk management practices, with special attention given to the ISO 31000 and COSO ERM frameworks. In addition, it highlights future trends in the field, setting the stage for identifying gaps in current methodologies and justifying the need for innovative solutions.

In the following chapter, the focus shifts to an in-depth analysis of risk management process frameworks. Here, the principles and procedures of ISO 31000:2018 and COSO ERM 2017 are reviewed and compared. Their respective strengths, challenges, and applicability to IT projects are examined in detail. The chapter concludes with a comparative perspective that emphasizes how these two widely adopted frameworks address risk across different organizational levels and project phases.

Building upon this analysis, the next chapter explores novel and emerging approaches to risk management. It investigates the role of digital twins, artificial intelligence, machine learning, and behavioural science in shaping more adaptive and dynamic risk strategies. These techniques are evaluated for their potential to complement or enhance existing frameworks, particularly in environments where unpredictability is a constant.

With these insights in place, the document then presents the development of a new risk management framework. This proposed model integrates both traditional methodologies and innovative techniques,

aiming to provide organizations with a practical and flexible tool for managing risk in IT projects. The framework's foundations, structure, and benefits are thoroughly explained, alongside recommendations for its implementation.

To validate the effectiveness of the framework, the following chapter outlines the evaluation process. It describes the methodology used for assessment, presents the results of its application, and discusses key findings. Strengths and areas for improvement are identified, along with comparative evaluations that position the proposed framework in relation to existing approaches.

The final chapter brings the dissertation to a close with a summary of the main findings, contributions to academic and professional knowledge, and reflections on the practical implications of the research. It also acknowledges the study's limitations and suggests avenues for future investigation, reinforcing the importance of continuous innovation in risk management practices for IT projects operating in uncertain conditions.

.

2. LITERATURE REVIEW

2.1 Risk

2.1.1 What is Risk?

What is risk? It is such a simple question. Risk has a very basic definition that almost anyone could answer. However, the answer is also at the root of most of the current problems and inefficiencies in risk management today. We believe that having a clear and consistent definition of risk that is understood throughout an organization is one of the simplest, yet one of the most beneficial steps that an organization can take to improve its risk management activities. If you look up risk in the dictionary you will find “the possibility that something bad or unpleasant will happen”. This definition is fine, but it leaves a lot to be desired for risk management purposes.

We also need to be aware that risk is not a four-letter word and is not to be avoided. Rather, it is to be managed and controlled(Dennis Cox, 2022).

Business enterprises must judiciously engage in risk-taking commensurate with their operational context, while concurrently implementing rigorous measures for the assessment and mitigation of such risks to ensure their congruence with stakeholder anticipations. The assertion that "risk" should not be regarded as a pejorative term implies that a categorical avoidance of risk is untenable within the operational paradigm of a business entity. It is inherently intrinsic to business operations to engage in calculated risk-taking endeavours.

We will divide the definition of risk into three parts, the first part being the element of uncertainty that is present. The second part is a future element, and the third part is an element that risk has both upside and downside components.

The initial facet of this delineation pertains to the presence of uncertainty. In short, within the domain of risk, there is an inherent element of unpredictability regarding future outcomes. The terms "risk" and "uncertainty" are often used interchangeably.

Both (Perminova 2008) and (Olsson 2007) argue that risk arises because of uncertainty in projects. (David Cleden 2009) agrees, stating that "uncertainty is the intangible measure of what we don’t know, risk is the statement of what may arise from that lack of knowledge". When we assert that a given scenario is characterized by uncertainty, we effectively imply that it includes some level of risk, and vice versa.

In the technical mathematical literature, as well as in the academic risk community, risk and uncertainty have close, but distinct meanings(Knight 1921). With risk, you have a range of possible outcomes, but the mathematical distribution is known(Aven 2013).

To illustrate the differences between risk and uncertainty, let us tackle the following examples.

Imagine a company that is considering introducing a new product. The company has historical data on similar product launches that allows it to estimate the potential sales volume, the likelihood of various levels of market acceptance, and the associated financial gains or losses. They can use this data to calculate the expected value of the product launch and decide whether the potential rewards outweigh the risks. This is a risk because the company can assign probabilities to the different outcomes based on experience.

Consider a technology startup operating in an emerging industry, such as space tourism. The industry is new, and there is no historical data to predict how the market will develop, what the customer demand will be, or how regulations might evolve. The startup faces uncertainty because it cannot accurately predict these outcomes or assign probabilities to them. They must adopt adaptive and flexible approaches to manage this uncertainty, as traditional risk management strategies are insufficient (Team, 2021).The second element of the definition is that it concerns the future. Despite of this being incredible obvious, too often we focus on the past and as a result we spend too little time creatively thinking about what might be. Risk cannot be managed in a rearview mirror, and while the past might be the precursor to the future, it is not a very reliable one(Rick Nason, 2022).

The professional risk should possess a deep understanding and reverence for historical context, while maintaining a keen focus on current circumstances and nurturing a forward-thinking imagination(David Cleden 2009). Again, there seems to be a disconnect as risk measures and risk strategies, as well as tactics are often criticized for fighting the last crisis, and since we cannot change the past, the best we can hope for is to manage the future.

The final element of our definition of risk is that risk includes both downside and upside. There is considerable disagreement in the literature as to whether the impact of a project risk must always be negative, or whether there is such a thing as positive risk. For example, (Chapman 2011), (David Cleden 2009) and (Morris 2013) argue that the term risk covers only those potential events that have negative impact on the project. Therefore, project risks are threats to the success of the project. In contrast, both PMI and APM, as well as a number of scholars (Larson 2011); (Lehtiranta 2014); (Perminova 2008)) take a broader view of risks, arguing that the impact of risks can be both positive and negative: positive

in the sense of providing new opportunities for the project, and negative in the traditional sense of threatening the achievement of one or more project objectives.

However, an equal focus on the upside is what makes all the difference in the future success of a project. Therefore, after careful consideration, we will adopt the dual nature of risk because this dual nature is critical to a balanced approach to risk management that seeks to capitalize on potential opportunities while mitigating threats. A comprehensive and nuanced definition of risk is fundamental to effective risk management in highly uncertain IT project environments. By considering the elements of uncertainty, future orientation, and the dual nature of risk, this dissertation can propose innovative approaches that enhance the ability of organizations to manage risks proactively and strategically. This balanced and futuristic perspective will be critical for navigating the complexities of modern IT projects.

2.1.2 Types of Risks

Cost Risk

Cost risk is probably the most common project risk of the bunch, resulting from poor or inaccurate planning, cost estimating, and scope creep. When this happens, project managers end up spending more money than they have on a project, which can hurt the business in other areas, or cause the project to go unfinished if funds and resources can't be replaced (Simplilearn 2023).

Schedule Risk

The result of poor planning, schedule risk is the risk that project tasks and activities will take longer to complete than estimated. Schedule risk is closely related to cost risk because any schedule slippage often increases costs, slows project benefits, and throws off schedules, losing any competitive advantage you may have at the outset (Megan Bell 2022).

Performance Risk

This project risk is not the fault of any one party, which makes it particularly daunting. Performance risk is simply the risk that the project won't deliver the results and benefits described in the project specifications. Even if you keep costs within budget and stay on schedule, performance risk can mean that you've wasted time and money on a project that ultimately failed to deliver (Simplilearn 2023).

Operational Risk

Focuses on how things are done within an organization and not necessarily what is produced or inherent in an industry. These risks are often associated with active choices about how the organization operates and what it prioritizes. While the risks are not guaranteed to result in failure, reduced production, or

increased overall costs, they are perceived to be higher or lower depending on various internal management decisions.

Because it reflects man-made procedures and thought processes, operational risk can be summarized as a human risk; it is the risk of business operations failing due to human error. It varies from industry to industry and is an important consideration in potential investment decisions. Industries with less human interaction are likely to have lower operational risk (Troy Segal 2023).

Communication Risk

Communication risk in a project refers to the potential for communication failures, errors, or misunderstandings that could lead to delays, rework, or even project failure. This risk can be caused by language barriers, cultural differences, technological limitations, or lack of clarity in messages(Project Management Institute 2017).

Scope Creep Risk

Scope creep risk in a project refers to the tendency for project requirements to expand beyond the originally defined scope. This can happen for a variety of reasons, such as changing stakeholder expectations, evolving business needs, or inadequate project planning. Scope creep can lead to delays, increased costs, reduced quality, and project failure(Kerzner 2017).

Skills Resource Risk

Skills resource risk in a project refers to the possibility that the project team does not have the necessary skills, knowledge, or expertise to successfully complete the project. This risk can arise from a variety of factors, including changes in project scope, unexpected technical challenges, resource availability, and turnover of key project team members.

The consequences of skills resource risk can be significant, including project schedule delays, increased costs, lower quality deliverables, and reduced stakeholder satisfaction. Therefore, it is essential to identify and manage skills resource risks effectively to ensure project success(Nicholas and Steyn 2020).

Market Risk

Market risk includes risks posed from competition, commodity markets, interest rates, foreign exchange, and liquidity and credit risks. This project risk is more unpredictable and difficult to plan for, but there are ways in which project managers can protect their business.(Simplilearn 2023)

Governance Risk

Governance risk is related to the performance of the board and management with respect to the community, ethics, corporate reputation, and community stewardship. This risk should be easier to

mitigate because it depends largely on the behaviour of the company's leaders. Of course, this risk is still real and should be taken seriously (Simplilearn 2023).

Strategic Risk

Strategic risk is another type of performance risk. Issues result from mistakes made when strategizing, such as picking project management software that doesn't work well for your project.

Legal Risk

Legal risks, arising from legal and regulatory duties, are inherently unpredictable. These encompass potential challenges like contract risks, lawsuits against the business or organization, and internal legal issues.

While these categories of risks are all critical to consider in project management, they do not operate at the same level of influence or severity. Some risks, such as cost risk and schedule risk, are highly tangible and can often be quantified and mitigated through improved planning and monitoring(Hillson 2009). Others, like market risk or legal risk, are more external and unpredictable, requiring adaptive strategies and contingency planning(Aven 2016). Meanwhile, risks such as communication risk, skills resource risk, and governance risk are closely tied to organizational culture and human factors, making them more complex to manage due to their qualitative and dynamic nature(Kutsch and Hall 2010). This layered hierarchy of risks underscores the need for a comprehensive, differentiated approach where project managers prioritize and tailor mitigation strategies according to the type, source, and potential impact of each risk.

2.1.3 What Causes Risks?

Unclear Project Objectives:

The lack of clear and unambiguous project goals and requirements can cause a variety of problems. When project goals are not well-defined, it can lead to misunderstandings among team members, stakeholders, and customers. This lack of clarity can lead to scope creep, where additional requirements are added without proper evaluation, impacting project schedules and resources.

Unclear project goals hinder the development of a cohesive project plan. Team members may interpret goals differently, leading to inconsistent efforts and potentially conflicting results. This lack of clarity makes it challenging to prioritize tasks and allocate resources effectively. Additionally, it opens the door to scope creep, where new requirements emerge throughout the project, impacting timelines and budgets (Schwalbe 2018).

Inadequate Planning:

Inadequate planning stems from shortcomings in estimating project requirements, allocating resources, and creating realistic schedules. Insufficient attention to these aspects can result in project delays, cost overruns, and increased risks. Effective planning is fundamental to project success and involves comprehensive assessments of the project scope, resource requirements, and potential challenges.

Inadequate planning often manifests in underestimated project complexities and timelines. Poor estimation of resource needs can lead to overburdened teams and compromised project quality. Scheduling discrepancies can result in missed deadlines, impacting the overall project timeline. Additionally, inadequate planning may lead to budget overruns, affecting the financial aspects of the project (Kerzner 2017).

Technology Complexity:

The complexity of IT systems, including emerging technologies and integration challenges, introduces technical risks. Software bugs, compatibility issues, and system failures may arise when dealing with intricate technologies. The rapid evolution of IT landscapes requires project teams to navigate and adapt to complex technological environments.

Technology complexity is inherent in IT projects, especially those involving cutting-edge technologies. Integration challenges may emerge when incorporating diverse systems, leading to compatibility issues. The development of software solutions within intricate frameworks can result in the discovery of unexpected bugs and errors. System failures can occur due to the interdependence of various components, requiring vigilant risk management (Sommerville 2011).

Inadequate Stakeholder Communication:

Poor communication with stakeholders, including customers, users, and team members, is a common cause of project challenges. Ineffective or missing communication can lead to misunderstandings, changing requirements, and unmet expectations. Stakeholder involvement is critical to project success, and inadequate communication can jeopardize the alignment of project goals.

Inadequate stakeholder communication often results in misinterpretations of project objectives and deliverables. This can lead to mid-project changes in requirements, causing disruptions and impacting timelines. Furthermore, unmet expectations among stakeholders may lead to dissatisfaction and strained relationships. Clear and consistent communication is essential for fostering collaboration and ensuring that all stakeholders are aligned with project objectives (Byron A. Love 2017).

Insufficient Resources:

Inadequate staffing, skill shortages, and resource constraints can significantly impede project progress. When project teams lack the necessary resources, including skilled personnel and sufficient budgets, the result can be increased workloads, compromised project quality, and heightened risks.

Insufficient resources may lead to overburdened project teams, impacting their ability to meet deadlines and deliver quality outcomes. A lack of skilled personnel can result in gaps in project capabilities, leading to delays and potential errors. Resource constraints, such as budget limitations, can hinder the adoption of necessary tools and technologies, affecting project efficiency (Heagney 2022).

2.1.4 The definition of Project Risk Management

The study of risk management began after World War II. Several sources ((Crockford 1982);(Williams and Heins 1964);(Niehaus and Harrington 2003)) date the origin of modern risk management to 1955–1964. Snider (1956) observed that at that time there were no books on risk management, and no universities offered courses in the subject. The first two academic books were published by (Mehr and Hedges 1963) and (Williams and Heins 1964). Their content covered pure risk management, which excluded corporate financial risk. In parallel, engineers developed models for managing technological risk. Operational risk partially covers technological losses; today, operational risk must be managed by firms and is regulated for banks and insurance companies. Engineers also consider the political risk of projects.

If risk encompasses the potentiality for both favourable and unfavourable outcomes, then the practice of risk management involves efforts to increase the likelihood and impact of positive risk events, while simultaneously taking actions to reduce the likelihood and magnitude of adverse risk events (Dionne 2013).

Risk management ensures that almost all problems are detected early enough to allow time to recover from them without missing schedules or exceeding budgets (J. Tamak and D. Binda 2013).

Elkington and Smallman(2000) claim that project risk management is essential for the project success. The authors conducted a study on a British utility company to assess its project risk profile. Based on the effects of risk, the authors developed a framework that might explain project success by: a) assessing the different types of project risks to measure the amount of risk management processes undertaken by a project manager, creating questionnaires to collect business risks, procurement risks, management risks and technical risks; b) assessing how and when the project manager applied risk management processes during the project; and c) determining the project managers' knowledge of and attitudes toward risk management. A total of 10 out 20 questionnaires were completed by the invited project managers. They

found that the most successful projects used more risk management practices. They also perceived that the earlier risk management is initiated, the more successful a project is (Peixoto et al. 2014).

A project risk management methodology typically provides a framework for identifying risks, performing both qualitative and quantitative assessments, developing response plans, and implementing monitoring mechanisms. By providing a comprehensive set of tools and techniques, the project manager is empowered to enhance the likelihood and impact of events that could provide opportunities for the project, while concurrently mitigating the probability and impact of those that might adversely affect the project objectives.

PMBoK® defines six risk management processes: plan risk management, identify risks, perform qualitative risk analysis, perform quantitative risk analysis, plan risk responses and control risks(Project Management Institute 2017).

The risk management plan prescribes the actions necessary to address project risks:

Risk Identification: This phase involves identifying and documenting potential risks that could impact project objectives.

Qualitative Analysis: This step subjectively assesses the likely consequences and likelihood of risks in subjective terms, which helps to prioritize risks.

Quantitative Analysis: Reserved for the most significant project risks identified in the qualitative analysis, this step involves a rigorous quantitative assessment of their likelihood and impact. This quantitative analysis aims to accurately measure the likelihood and impact of high-priority risks.

Plan Risk Response: Planning helps to develop actions to enhance opportunities and to reduce threats to project objectives (PMI 2013).

Control Risks: Establishing a ranking system is imperative because it is difficult, if not impossible, to formulate a comprehensive plan to address every conceivable risk at every stage of a project. By assigning a risk factor value to each identified risk, the project team gains a strategic guide for mitigating project risks, focusing on developing contingency plans only for tasks associated with the highest risk factors.

While it is common practice is for project teams to focus their risk mitigation efforts on the top 20 percent of identified risks, it is recognized that this guideline is not rigid. Barki (2001) emphasizes the need to adjust a project's risk management profile based on the inherent risk level of the project itself. Projects with higher inherent risk may require more extensive risk mitigation efforts.

Additionally, the risk management plan should encompass the specification of appropriate tools and techniques tailored to each stage of the risk management process, aligning with the unique requirements of a particular project or project type.

Some studies indicate that project risk management approaches are not widely accepted in project management because of the time required to apply them, the difficulty in obtaining input estimates and assessing risk probabilities, human/organizational resistance to change, difficulty in understanding and interpreting the results of the risk management process, and finding appropriate risk management methods(H. M. Leung, 1998). However, a 2013 worldwide survey study, conducted by G. Fernandes, et. al (2013), derived from the analysis of 68 surveyed project management tools and techniques, found that certain knowledge areas such as risk, scope, time, communication, and integration have a notable importance among the most valuable project management practices. Each of these areas includes at least three project management practices in the top 20 of the lists. For example, in the area of risk management, practices such as "risk identification", "risk response plan", and "qualitative risk analysis" were identified. Interestingly, none of the tools associated with cost or quality, which are typically linked to project objectives, ranked in the top 20 of the lists.

Considering the above, project risk management emerges as an integral facet of overall project management, effectively addressing both uncertainties and identified risks inherent in the project. As a result, it provides valuable information that can be used to optimize the decision-making process.

2.1.5 Risk Management Strategies

Any organization, regardless of scale or industry, can benefit from implementing a systematic approach to address potential threats through a risk management strategy. Rather than viewing risk management as a series of isolated tasks, it is more beneficial to view it as an iterative process. In this continuous cycle, both new and existing risks require ongoing identification, analysis, management, and monitoring. This approach facilitates a perpetual evaluation and response mechanism, guaranteeing the perpetual safety of the company(Project Management Institute 2017).

In the field of risk management, various strategic approaches are used to address identified risks. One such approach is Risk Acceptance, where risks are acknowledged and accepted without intervening to prevent their occurrence. This approach is based on the premise that the cost of eliminating certain risks may outweigh their initial impact. Confidence in effectively managing the risk if it materializes is crucial for the success of this strategy. Sometimes the cost of mitigating risks can exceed the cost of the risk itself, in which case it makes more sense to simply accept the risk. After all, why spend £200,000 to prevent a £20,000 risk? However, this approach does come with a gamble. You will need to be sure that, if the risk does occur in the future, then you will be able to deal with it when the time comes. For this

reason, it is best to only accept risks if the risk has a low probability of occurring or if the impact will be minimal if it does occur (Dennis Cox 2022).

Another strategy is Risk Transfer, in which the responsibility for managing risk is delegated to an external entity. Although the risk persists, another organization assumes the obligation to manage and mitigate its impact. Insurance mechanisms are often an example of this approach.

Risk Avoidance, on the other hand, advocates steering clear of identified risks altogether or eliminating their potential occurrence. This strategy is advisable when the potential impact of a risk carries significant repercussions for the organization. However, exercising caution is essential to avoid forgoing valuable growth opportunities. An illustrative example of risk avoidance occurs in the area of investments. After a comprehensive risk analysis of a potential investment, if the perceived risks are deemed too high, the strategic choice is to abstain from the investment altogether.

It is imperative that risk avoidance be applied selectively, reserving this strategy for risks that have the potential to have a significant impact on the organization. However, a careful balance is required, as an indiscriminate avoidance of every identified risk could result in missed positive opportunities. There remains the inherent uncertainty that an investment foregone because of perceived risk could have yielded favourable returns. Therefore, careful risk analysis is paramount to ensure that decisions are based on informed judgments that weigh potential risks against potential opportunities (Rick Nason 2022).

A widely accepted approach is Risk Reduction, which involves actively mitigating risks through preventive measures or interventions designed to prevent their occurrence or minimize their impact. This method enables organizations to adopt measures and tactics, such as the implementing quality management systems to reduce manufacturing defects. Risk reduction, a prevalent strategy in risk treatment, is synonymous with the concept of lowering risk. Choosing for this approach entails devising measures or actions aimed to make risks more manageable.

In manufacturing, a prime example of risk reduction involves addressing the risk of products being produced to incorrect specifications. Implementing a quality management system is an effective way to reduce the likelihood of such occurrences and is an example risk reduction.

Similarly, in the financial industry, the challenges associated with new regulations can present risks. Mitigating the risk of non-compliance can be achieved by implementing a digital solution tailored to manage regulatory requirements. This strategic use of technology serves as a practical example of risk reduction, demonstrating the ability to minimize potential negative impacts associated with regulatory changes (Rick Nason 2022).

The selection of a specific risk management approach (Figure 1) is critical in determining the organization's ability to effectively manage and control potential risks. The strategy chosen will have a profound impact on whether the organization can proactively manage each risk or, conversely, remain vulnerable to potentially catastrophic consequences. This strategic decision-making process is an integral part of the overarching risk management framework and shapes the organization's resilience and adaptability in the face of a constantly evolving risk landscape.

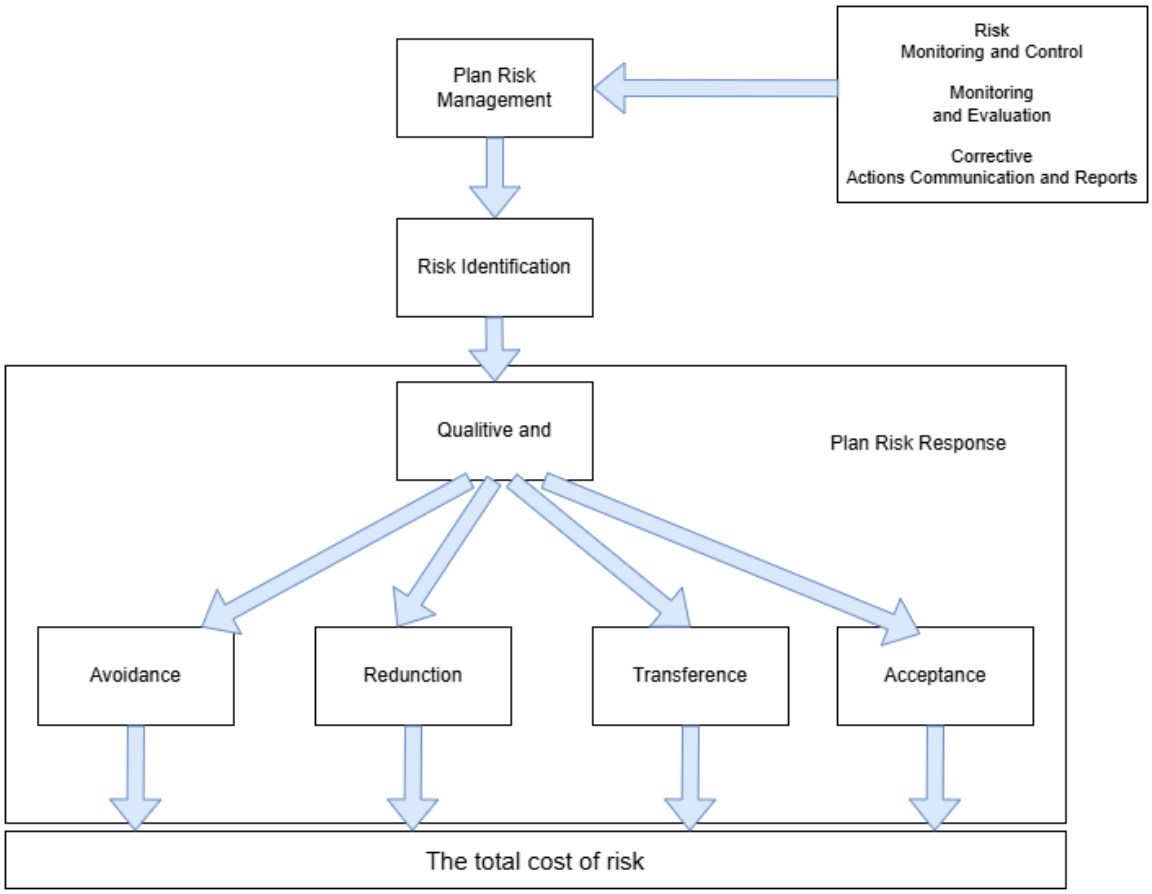


Figure 1- The relationship between the stages of the risk management

2.2 The Concept of Uncertainty in IT projects

Uncertainty in IT projects refers to the lack of complete certainty about various aspects of the project, including its outcomes, processes, and environment. It is characterized by unknown factors that may affect the project, but which cannot be predicted or measured with precision. This uncertainty can arise from a variety of sources such as technological changes, market conditions, regulatory environments, and resource availability (Fahad Usmani 2024).

2.2.1 Impact on risk management

The impact of uncertainty on risk management in IT projects is significant. While risks can often be identified, quantified, and managed through proactive planning and mitigation strategies, uncertainties present a more complex challenge because they cannot be easily measured or anticipated. This makes it difficult for project managers to develop a response plan to effectively manage these uncertainties.
Uncertainty in IT projects can take several forms (Wrike Team 2023) :

- Technological Uncertainty: Rapid advances in technology can render existing project plans obsolete, and new software or hardware can present unforeseen challenges.
- Market Uncertainty: Fluctuations in customer preferences, competition, and economic conditions can affect the viability and success of IT projects.
- Regulatory Uncertainty: Changes in laws and regulations can impact project scope, schedule, and cost, creating challenges in compliance and planning.
- Resource Uncertainty: The availability of skilled personnel, budget constraints, and time limitations can introduce uncertainty into project timelines and deliverables.

Several strategies can be used to manage uncertainty in IT projects (Dmitriy Stepanov, 2023):

- Agile Methodologies: Agile practices such as Scrum or Kanban promote adaptability and flexibility, allowing teams to respond quickly to changes and uncertainty.
- Continuous Planning and Refinement: Regular planning sessions help teams refine project requirements and goals, minimize misunderstandings, and provide clearer direction.
- Effective Communication: Establishing clear communication channels ensures that all stakeholders have a common understanding of project objectives, progress, and potential risks.
- Risk Management: Implementing risk management practices, such as conducting risk assessments and creating contingency plans, helps anticipate and manage uncertainty.
- Leverage Technology: Using project management software and data analytics can improve risk identification and monitoring.
- Scenario Planning: Preparing for multiple potential futures can help project managers develop flexible long-term plans that can adapt to changing circumstances

.

2.3 Main Frameworks

The two main risk frameworks used by organizations are the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the International Organization for Standardization's ISO 31000(TechTarget 2023).(Sityata and Dubihlela 2021)

Both frameworks exhibit substantial similarities, albeit employing slightly different structures and language nuances. They share common ground in recognizing the imperative need for a clearly articulated risk management objective. In addition, both frameworks include key elements such as risk identification, risk assessment, ongoing risk monitoring and communication. Crucially, they emphasize the understanding that risk management is a perpetual and continuous process. Both the COSO and ISO frameworks, as well as the various frameworks offered by the various risk management consultants, have attractive features. For organizations venturing into risk management for the first time, these frameworks offer an expedited initiation process. They serve as a quick way to get risk management practices up and running and to start a substantive discourse on the subject. In fact, these frameworks will stimulate a deeper conversation about risk management than many organizations may be prepared for. The comprehensiveness of the frameworks has the potential to move organizations quickly into action, causing them to assess their current risk management practices against these comprehensive frameworks, potentially leading to a sense of urgency or realization.

2.3.1 ISO 31000

The ISO 31000 Risk Management Standard is an international standard that provides guidelines for managing the risks faced by organizations. It enables organizations to apply risk management to all strategic, managerial, and operational tasks, as well as to projects, functions, and processes (International Organization for Standardization 2018). Developed by the International Organization for Standardization (ISO), the standard is designed to be used by organizations of all sizes and is equally applicable to the public and private sectors. The ISO 31000 standard is based on three main components: principles, framework, and risk management process. It outlines a generic approach to risk management that can be applied to different types of risks and used by any type of organization (Alexander S. Gillis 2023). The standard provides a consistent vocabulary and concepts for discussing risk management. The risk management process outlined in the ISO 31000 standard includes activities such as risk identification, analysis, evaluation, and treatment. The primary goal of ISO 31000 is to help organizations protect their assets, achieve their objectives, and improve decision-making. By implementing the ISO 31000 standard,

organizations can improve their efficiency, decision-making, and the achievement of organizational goals. It also helps protect assets and reputation, ensure regulatory compliance, and improve competitiveness and growth.

ISO 31000:2018 is the most recent version of the standard. There are also other risk management standards, including the ISO IEC 31010 standard for risk management from ISO and the International Electrotechnical Commission.

ISO 31000 framework and guidelines

The risk management framework consists of the following six distinct areas as we can see on fig. 2:

Leadership. Leaders within the organization must take the initiative to ensure that ISO 31000 is adopted and applied in a way that is consistent with the organization's culture and business objectives.

Integration. While it's important to integrate risk mitigation into as many organizational processes as possible, it's important not to cause operational bottlenecks or stand in the way of core business processes being performed.

Design. Organizations must design a risk management strategy based on their needs.

Implementation. The implementation process integrates the organization's risk management design into business processes. Implementation is usually a formal process with stated objectives, deadlines and reporting requirements.

Evaluation. Evaluation assesses the design to determine what is working and what may need to be refined.

Improvement. Organizations should continuously look for ways to improve their ISO 31000 implementation.

The ISO 31000 framework may be structured differently depending on the organization and its decision on how to implement the standard. For example, an organization can follow ISO 31000 using the following six guidelines: Scope, Normative References, Terms and Definitions, Principles, Framework and Process (Alexander S. Gillis 2023).

ISO 31000's risk management principles

ISO 31000 seeks to help organizations take a methodical approach to risk management by doing the following three key things:

- Identifying risks.
- Evaluating the probability of an event tied to an identified risk occurring.
- Determining the severity of the problems caused by the event occurring.

As such, ISO 31000 doesn't seek to eliminate risks, as the total removal of all risks is impossible. Instead, it's designed to help organizations identify their risks and develop a strategy to mitigate or reduce them where appropriate.

The following eight core ISO 31000 principles are the foundation for establishing a risk management framework:

- Embrace inclusiveness: Successful efforts demand the active involvement of key stakeholders, considering their knowledge and perspectives. Ensure transparency in risk management and avoid confusing jargon for better understanding.
- Stay dynamic: Organizations evolve, requiring continuous risk analysis. What's relevant today may change tomorrow. Ongoing assessments is critical to maintaining effective risk mitigation,
- Rely on the best information: Base risk mitigation on the most current and accurate information available to stakeholders. Acknowledge the impossibility of having all necessary information you need and anticipate the existence of unforeseen risks.
- Consider human and cultural aspects: Human behaviour and organizational culture play a role in risk management. Include risks associated with human error and the organization's unique culture in the identified risks.
- Strive for continual improvement: Adhering to ISO 31000 principles involves embracing continuous improvement, ensuring that risk mitigation efforts enhance over time.
- Foster integration: Integrate the concepts of risk mitigation and identification into all business processes for a consistent approach.
- Be structured and comprehensive: Develop a comprehensive risk mitigation strategy that addresses all known risks, ensuring a structured and thorough approach.
- Customized. Because each organization is unique, the concepts of ISO 31000 should be tailored to the organization to achieve its objectives.



Figure 2-The ISO 31000 guideline (Rouse 2023)

The ISO 31000 risk management approach has two key components:

The Framework

The ISO 31000 Framework is modelled after the Plan, Do, Check, Act (PDCA) cycle, which is used to create all management systems. "This Framework is not designed to prescribe a management system, but rather to help the business integrate risk management into its overall management system", according to the ISO (Riskonnect n.d.). This remark should encourage organizations to be flexible in integrating framework parts as needed.

The major components of the framework (Figure 1) include the following (ISO 2018):

- Governance and policy. Establishes the mission and displays the organization's commitment.
- Program design. Design of the overarching framework for continuous risk management.
- Implementation. Putting the risk management framework and program in place.
- Monitoring and evaluation. Oversight of the structure and performance of the management system.
- Continuous Enhancement. Enhancements to the overall management system's performance(Riskonnect n.d.).

Organizations, particularly those with no experience with management systems, should plan to spend significant time developing a solid framework and resist the temptation to go right into the risk assessment process. Process design is critical because the Framework offers the consistency and continuity needed to develop a program rather than merely completing a project (RiskOptics 2023).

The Process

An organization is ready to construct the Process after creating the risk management Framework. ISO 31000(International Organization for Standardization 2018) says the process is “multi-step and iterative; meant to identify and assess risks in the corporate environment.”

Regular communication is crucial early in the Process for understanding stakeholders’ interests and concerns and thereby confirming the Process’s emphasis. Later, ongoing communication aids in conveying the reasoning behind decisions and why the organization needs certain risk mitigations(RiskOptics 2023).The ISO 31000 Risk Management Standard provides organizations with a generic approach to risk management that can be applied to different types of risks and used by any type of organization. It outlines a risk management process that includes activities such as risk identification, analysis, evaluation, and treatment. The standard emphasizes the importance of continuous monitoring and review to ensure that the organizations is responding to changes in the risk environment and that controls are functioning properly. ISO 31000 also highlights the significance of setting the "context," which involves evaluating the organization’s internal and external surroundings as they relate to corporate goals and tactics. This context-setting process is essential to a comprehensive risk assessment, which includes the identification, analysis and evaluation of specific risks. The standard aims to help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats, and effectively allocate and use resources. It provides a universal standard for practitioners and companies employing risk management, offering a level of reassurance in terms of economic resilience, professional reputation, and environmental and safety outcomes.

2.3.2 COSO ERM

The COSO Enterprise Risk Management (ERM) Framework, updated in 2017 by the Committee of Sponsoring Organizations of the Treadway Commission, is a comprehensive guide used by organizations worldwide to improve their risk management practices (Alexandria Claypole 2021). It emphasizes the integration of ERM with strategic objectives and corporate culture, covering eight key components: internal environment, goal setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring activities. The framework aims to provide a holistic approach to managing risk and performance, going beyond traditional internal controls to offer tools for evaluating systems and providing assurance to stakeholders (Alexandria Claypole 2021). At its core, ERM is about maximizing value for stakeholders by managing the balance between risk and opportunity in the face of uncertainty. It advocates for an enterprise-wide assessment of risks, moving away from isolated

risk management to a comprehensive, portfolio view that considers the overall impact of risks on the organization. This strategic approach helps organizations not only in identifying and managing risks but also in seizing opportunities, thereby enhancing their ability to create and preserve value.

Under the COSO framework(fig. 3), ERM is geared to achieving an entity's objectives, set forth in four categories:

- Strategic - These objectives are high-level and are aligned with an entity's mission.
- Operations - These objectives refer to the effective and efficient use of resources.
- Reporting - These objectives surround an entity's need for reliable reporting.
- Compliance - These objectives refer with an entity's need to comply with applicable laws and regulations.

Managing risks in these four categories within an entity's risk appetite will aid in the creation of stakeholder value (Enterprise Risk Management Initiative Staff 2004).



Figure 3-COSO ERM Framework
(Committee of Sponsoring Organizations of the Treadway Commission 2017)

Internal environment

The internal environment of an organization plays a crucial role in shaping its approach to risk management and ethical values. The board of directors, as the ultimate decision-making body, is responsible for setting the tone and providing leadership on risk management. An unbalanced board that lacks appropriate expertise and diversity may struggle to set the right tone, potentially undermining the organization's risk management efforts. Additionally, the effectiveness of board committees, particularly the audit and risk committees, can significantly influence the overall risk management tone within the

organization (Institute of Risk Management 2017). Furthermore, the example set by the board may be compromised by shortcomings in the management of various divisions or business units. Inadequate mechanisms for controlling line management, lack of awareness of responsibilities, or failure to prioritize responsible risk management over purely achieving results can all contribute to a weakened risk management culture. Critics of the Enterprise Risk Management (ERM) model have argued that it places too much emphasis on the internal environment, neglecting the influence of the external environment, such as competitive pressures, regulatory requirements, and the impact of external stakeholders, on risk appetite and management culture (Christophe Veltsos 2017).

This criticism suggests that the ERM model should more comprehensively consider the broader external factors that shape an organization's approach to risk. Thus, the internal environment is a critical factor in determining an organization's approach to risk management and ethical values. While the board sets the tone, it is essential that all levels of the organization are aligned in their understanding and management of risk, and that the ERM model considers the broader external influences on risk management and culture.

Five Key Components of the COSO ERM Framework

The COSO ERM 2017 framework consists of five interrelated components, as we can see in figure 3, with a total of 20 principles spread throughout each component. The five components are (Committee of Sponsoring Organizations of the Treadway Commission 2017):

1. Governance and Culture: This component focuses on the importance of effective governance and the role of organizational culture in supporting risk management.
2. Strategy and Objective-Setting: This component emphasizes the integration of risk management with strategy and objective-setting, highlighting how ERM should be a strategic tool.
3. Performance: This component deals with identifying, assessing, responding to, and reporting on risks in the context of achieving strategy and business objectives.
4. Review and Revision: This component involves evaluating the ERM process and making necessary revisions based on performance insights.
5. Information, Communication, and Reporting: This component underscores the need for ongoing identification and sharing of risk and strategy information throughout the organization.

2.4 Future Trends

The future of risk management is being shaped by emerging trends and technologies that are revolutionizing traditional practices. These trends are poised to significantly alter the risk landscape, creating new opportunities and challenges for risk leaders and organizational leaders alike.

Some of the key emerging trends in risk management include(Julien Haye 2024; TechTarget 2023):

- Maturity and risk capability
- Artificial Intelligence and Big Data
- Pervasive Controls
- Application of Behavioural Science
- Collective Risk Management
- Digital Twins

These trends are reshaping the enterprise risk management landscape and influencing the way organizations approach risk management. As the business environment continues to evolve, it is crucial for organizations to stay ahead of these emerging trends and leverage them to their advantage. By embracing these trends, organizations can navigate uncertainties, maintain resilience, and create value through effective risk management practices.

Maturity and Risk Capability

The recognition of different levels of maturity and risk capability in organizations is a significant trend in risk management. Risk maturity reflects how well an organization integrates risk management into its culture, processes, and decision-making, while risk capability refers to the organization's proficiency in identifying, assessing, responding to, and monitoring risks. Depending on these levels, organizations may require varying tools, methods, and frameworks to manage risks effectively. For IT projects, which often face high uncertainty, aligning with the Factor Analysis of Information Risk (FAIR) framework can be particularly beneficial. The FAIR framework helps quantify IT and cyber risks in financial terms, aiding in decision-making around risk initiatives (Nghi M. Nguyen n.d.). The 5-phase risk maturity model outlines the progression from a basic, reactive approach to risk management to a sophisticated, proactive strategy:

- Ad-hoc Stage: Characterized by a reactive approach with minimal understanding or management of risk.
- Preliminary Stage: Risks are acknowledged but managed in silos with limited process discipline.

- Defined Stage: A common risk assessment framework is in place, providing an organization-wide view of top risks.
- Integrated Stage: Risk management activities are coordinated across the business, utilizing common tools and processes for enterprise-wide risk monitoring.
- Optimized Stage: Focus shifts from managing a list of risks to embedding risk considerations into strategic planning and decision-making, aiming for the achievement of objectives.

The FAIR framework, particularly at higher maturity levels, enables IT projects to quantify risks and make informed decisions, thereby managing the uncertainties inherent in technology projects more effectively. This approach emphasizes the importance of evolving risk management practices to align with organizational objectives and the specific challenges of IT projects (Proença et al. 2017).

Artificial Intelligence and Machine Learning

The landscape of risk management is undergoing a transformation with the integration of artificial intelligence and machine learning, offering advanced analytics capabilities. These technologies empower organizations to analyse extensive datasets, recognize patterns, and make informed, data-driven decisions. In real-time, AI and ML algorithms can evaluate risks, identify anomalies, and automate risk assessment procedures, thereby elevating efficiency and precision in risk management practices.

The infusion of AI into risk management is reshaping how businesses anticipate, analyse, and address various uncertainties. By leveraging artificial intelligence for risk management, companies are not only increasing operational efficiency but also refining the precision of their risk assessment strategies.

Where is this trend already in play?

Warwick Analytics' early warning and prevention system looks hours, days, and months ahead to try to predict when and how products in the field (such as aircraft and vehicles) will require maintenance. Identifying the root causes of failure helps engineers take corrective action, such as remanufacturing and redesigning products. Economic benefits can include enhanced efficiency of plant or production line, reduced energy bills, and increased product life cycle. Hong Kong-based venture capital firm Deep Knowledge Ventures has appointed a software algorithm, "VITAL," to its Board of Directors. Just like other members of the board, VITAL gets to vote on whether the firm should make an investment in a specific company or not. It makes its decisions by scanning prospective companies' financing, clinical trials, intellectual property, and previous funding rounds. Nexgate is a provider of Deep Social Linguistic Analysis (DSLA) technology and natural language processing (NLP) based social media risk management tools.

Its major solutions scan social networks to try to discover and track an organization's accounts; detect fraudulent social media accounts, unauthorized changes, and anomalous behaviour on social account profiles; reduce potential liability from inadvertent posting of sensitive data; and demonstrate compliance with more than 35 standards and industry regulations (Albinson, Blau, and Chu n.d.).

Pervasive controls

Pervasive controls offer a strategic approach to risk management in IT projects, leveraging real-time data and hyper-connectivity to proactively manage risks. This method enhances operational efficiency, ensures compliance, fosters innovation, and builds trust by integrating risk management into the organization's infrastructure. To successfully implement pervasive controls, organizations should assess their risk management maturity, tailor controls to specific project needs, prioritize data protection and ethical practices, and continuously update their risk management strategies. This approach enables organizations to navigate the uncertainties of IT projects effectively, ensuring resilience and competitive advantage in the digital landscape (Debashis Saha and Amitava Mukherjee 2003).

Where is this trend already in play?

Saia, a US-based freight company, has worked with Intel to deploy sensors into its truck fleet to track maintenance needs, driver safety, fuel usage, and other metrics in real time. Through real-time process intelligence, this initiative has led to a 6 percent increase in fuel efficiency, which translated to $15 million in savings for Saia. In addition to achieving cost savings, Saia has been able to track maintenance needs, driver safety, and fuel usage, as well as other metrics, in real time. Fujitsu has developed wearable tags that can detect whether users have changed location or posture, have fallen down, or are experiencing high heat. With the help of these tags, employers can—in real time—monitor employees' working conditions or detect if they are carrying a heavy load or standing in a place where they might fall. The aim is to reduce the risks of injury at the workplace. Singapore-based TrustSphere, whose clients include financial services firms, specializes in trying to uncover the relationships that an employee has through digital interactions— attempting to reduce the risks of illegal collusion and internal fraud (Albinson et al. n.d.).

Application of Behavioural sciences

Incorporating behavioural sciences into IT project management can mitigate risks associated with high uncertainty by focusing on user engagement and retention. Behavioural scientists apply their understanding of habit formation to design products that keep customers returning, which is crucial for

long-term success and cost-effective customer acquisition. They also provide insights into team dynamics and recruitment strategies to reduce attrition and increase productivity. Furthermore, by identifying and addressing potential behavioural biases, they enhance decision-making processes. Cognitive biases, such as confirmation bias, groupthink, availability bias, anchoring bias, status quo bias, and hindsight bias, can significantly affect risk identification and assessment (VinciWorks 2018). These biases can lead to the overlooking of critical risks, misjudgement of risk probabilities and impacts, and resistance to acknowledging or adapting to new information. By recognizing these biases, risk managers can develop strategies to mitigate their influence (Gertner, Zaromb, and Roberts 2016).

This multidisciplinary approach ensures that IT projects are not only technically sound but also resonate with users and adapt to market demands, thereby reducing the risk of project failure and fostering sustainable growth (Abrachan Pudussery 2020).

Where is this trend already in play?

Fujitsu has built a platform that uses psychological profiling to ramp up computer security in the workplace. This enterprise tool aims to identify workers who are most vulnerable to cyberattacks and also gives advice on how to sidestep them, based on their behaviour while checking and sending emails, and browsing the web. This was developed after consulting social psychology experts and surveying more than 2,000 Japanese users, half of whom had experienced attacks, to determine which traits make some users more vulnerable to viruses, scams, and data leaks. Mi3 Security (formerly MetaIntell), a cloud based mobile risk management company, recently brought onboard a behavioural science expert as a technical solutions and business advisor in the office of the CEO. Hand hygiene company DebMed offers an electronic hand hygiene compliance monitoring system that seeks to measure the compliance level of an entire unit instead of individual performance. It predicts expected hand hygiene opportunities by considering unique conditions of each hospital unit, such as census and nurse-to-patient ratio. This aims to promote a spirit of collaboration and accountability while also providing actionable feedback for the group without singling out individuals (Albinson et al. n.d.).

Collective risk management

Collective risk management, exemplified by beta testing, bug bounty programs, and collaborative platforms like ThreatExchange and Wikistrat, offers a strategic approach to mitigating risks in IT projects with high uncertainty. These methods leverage the collective expertise of diverse groups, from end-users to security professionals, to identify and address potential vulnerabilities and threats before they impact

the project. Beta testing allows for real-world product testing, while bug bounty programs incentivize the discovery of security flaws, enhancing system robustness (HackerOne 2024).

Collaborative platforms facilitate the sharing of cyber threat information and strategic forecasting, enabling organizations to proactively manage complex risks. This collective approach not only improves product quality and security but also fosters innovation, ensuring the success of IT projects in rapidly changing environments.

Where is this trend already in play?

United Airlines is seeking to harness the power of the crowd to improve security of its software through a "bug bounty" program that will award miles to people for finding vulnerabilities. With this program, the company is following the steps of technology corporations like Google, Facebook, and Microsoft, which have their own bug bounty programs. These programs engage independent researchers, experts, and hackers to find potentially dangerous security flaws for a reward. ThreatExchange, a social data exchange platform by Facebook, is being used by security professionals and researchers across the world to share cyber threat information. Wikistrat, the crowdsourced consulting organization, uses interactive role-playing games that leverage a crowd of experts from all over the world for strategic forecasting. Wikistrat's open-source platform provides access to vetted crowdsourced expertise to address complex client issues and risks and to develop effective action plans (Albinson et al. n.d.).

Digital Twin

Digital twin technology is part of the rise of new digital technologies that support digital transformation by providing capabilities to enable new business models and decision support systems. Many organizations have already incorporated or are in the process of incorporating data, information, and analytics capabilities as part of their service offerings.

Concept

The concept of a Digital Twin originates from Michael Grieves' 2003 presentation on product life-cycle management based on his work with John Vickers. Grieves and Vicker' motivation for developing the concept was to shift from the predominantly paper-based and manual product data to a digital model of the product which would become foundational for life-cycle management. Similar concepts such as Cyber Physical Systems (CPS) and Internet of Things (IoT) all focus on the idea of connecting a physical system to data collection, computational and/or communication systems, but approaching it from differing perspectives: CPS concept from the system engineering and control perspective, IOT from a networking

and IT perspective, and Digital Twin from a computational modelling (machine learning/artificial intelligence) perspective (VanDerHorn and Mahadevan 2021).

Grieves provided the first characterization of the Digital Twin concept by stating that it consisted of three components, a physical product in Real space, a virtual representation of that product in the Virtual space, and the connections of data and information that tie the virtual and real products together. Over the past two decades, the interest in Digital Twins has grown across many industries and this has led to a wide variety of definitions and characterizations that have diluted Grieves' original description, to which this paper seeks to return and generalize.

Digital Twin characteristics

Using the generalized definition proposed above, the Digital Twin can be characterized by three primary components, as we can see in figure 4: A physical reality, a virtual representation, and interconnections that exchange information between the physical reality and virtual representation shown (VanDerHorn and Mahadevan 2021).

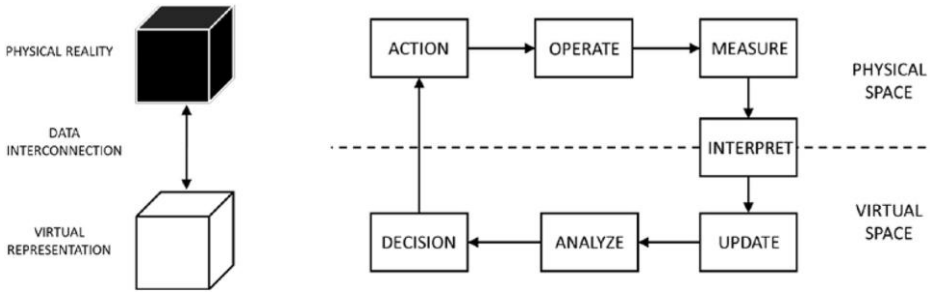


Figure 4- Digital Twin components and high-level processes.

(Grieves 2017)

3. Risk Management Process Frameworks

This chapter explores the key components, principles, and applications of ISO 31000:2018 and COSO ERM 2017 frameworks in the context of risk management. By examining these frameworks in detail, organizations can gain a deeper understanding of how to effectively identify, assess, and respond to risks, ultimately enhancing their resilience and ability to achieve their strategic objectives in an uncertain and dynamic environment. In this chapter, we will also compare both frameworks to gain a deeper understanding of their advantages and disadvantages. In the future, we will explore new approaches to improve these frameworks and our approach to risk management.

3.1 Risk Management in ISO 31000-2018

The risk management process outlined in ISO 31000 comprises five primary stages (fig. 5). Although depicted in a sequential manner in the image below, these stages are typically implemented iteratively in practice. This iterative approach allows for the identification, comprehension, and modification (if necessary) of risks in accordance with risk criteria established by the organization itself as part of the process.

Risk management process is often presented as sequential steps, in practice they are iterative activities.

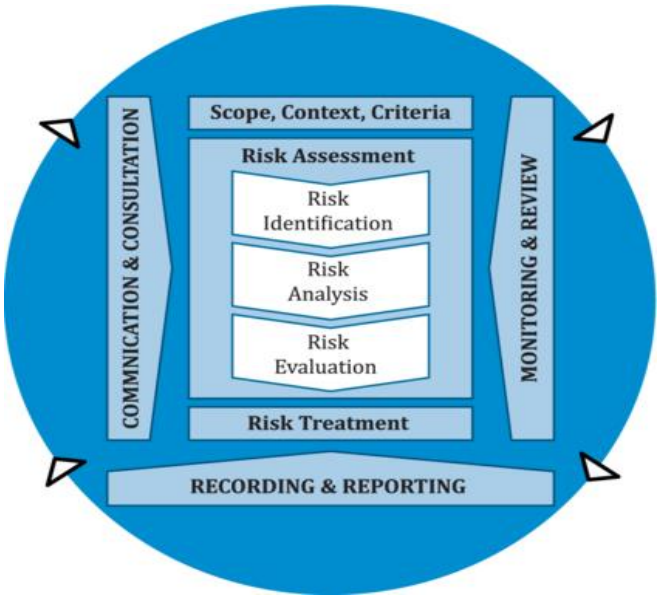


Figure 5-ISO 31000-2018 Process
(International Organization for Standardization 2018)

3.1.1 Processes in ISO 31000-2018

Communication and consultation

Effective communication and consultation are essential to ensure that those responsible for identifying and managing risks and those with a vested interest understand the basis on which risk-informed decisions are made and reasons why particular actions and treatments are selected.

The purpose of communication and consultation is to help relevant stakeholders understanding risk, the basis for decision-making, and the reasons for selecting particular actions. It is a continual and iterative process to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk.

A stakeholder is a person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making.

Consultation is a two-way process of informed communication between an individual or organisation and its stakeholders on an issue before deciding or determining a direction on that issue. It is:

- a process which impacts a decision through influence rather than power; and
- an input to decision making, not joint decision making.

Close collaboration between stakeholders is essential to facilitate the exchange of information that is factual, timely, relevant, accurate, and comprehensible, while also upholding the confidentiality, integrity, and privacy rights of individuals. This exchange of information encompasses various facets of risk management, including its identification, nature, likelihood, significance, evaluation, acceptability, and mitigation strategies.

Effective communication and consultation with both internal and external stakeholders should be seamlessly integrated into all phases of the risk management process. By fostering a shared understanding of perspectives and actively involving stakeholders in decision-making processes, such an approach enhances risk management practices.

A collaborative and consultative framework is instrumental in:

- Help establish the context appropriately and ensure that the interests of all stakeholders are understood and considered.
- Ensure that uncertainties, risks, issues and opportunities are adequately identified and managed.

- Bring together different areas of expertise when assessing or analysing risks to ensure different, and sometimes opposing, views are appropriately considered when defining the risk criteria and when assessing risks.
- Help secure endorsement, support and commitment for a treatment plan.
- Enhance any change management processes associated with making risk-informed decisions.

Methods of communication and consultation may include meetings, reports, on-line communication systems and learning packages, newsletters and flow charts (Barafort, Mesquida, and Mas 2019).

Scope, context and criteria

The purpose of establishing the scope, the context and criteria is to customise the risk management process and enabling effective risk assessment and appropriate risk treatment.

Defining the scope

You should define the scope of your risk management activities.

As your risk management activities may be applied at different levels (e.g., strategic, operational, programme, project, or other activities), it is important to be clear about the scope under consideration, the relevant objectives to be considered and their alignment with your objectives.

When planning the approach, considerations include:

- Objectives and decisions that need to be made.
- Outcomes expected from the activities.
- Time, location, specific inclusions and exclusions.
- Appropriate risk assessment tools and techniques.
- Resources required, responsibilities and records to be kept.
- Relationships with other projects, processes and activities.

The external and internal context pertains to the setting in which an organization defines and pursues its objectives. It is imperative that the context for risk management endeavours be delineated based on a comprehensive understanding of both the external and internal environments within which the organization operates. This contextual framework should be tailored to the specific circumstances in which risk management initiatives will be implemented.(Patrick 2024)

Establishing this context serves as the cornerstone for conducting risk assessments, providing a structured foundation that ensures clarity regarding the rationale behind such assessments. Additionally, it furnishes the necessary backdrop against which risks can be discerned and evaluated within the organizational landscape.

Understanding the context is important because:

Risk management takes place in the context of your objectives and activities.

- Your individual, team or organisational factors can be a source of uncertainty, risk and opportunity.
- The purpose and scope of the risk management process may be interrelated with your objectives.

Defining Risk Criteria

Risk criteria define the boundaries within which risks are considered acceptable in relation to organizational goals. Acting as a benchmark for risk assessment, they help determine whether a risk or opportunity aligns with the organization's objectives and risk appetite(International Organization for Standardization 2018).

These criteria assist in:

- Determining acceptable levels of risk across different objectives.
- Defining performance thresholds to assess variations that can be tolerated.
- Adapting evaluation methods based on the type of risk (e.g., financial vs. safety risks).
- Prioritizing risks by comparing them against predefined thresholds.
- Considering broader elements like legal, ethical, and sustainability factors, as well as stakeholder perspectives, control effectiveness, and the timing and cost of potential consequences.

Risk criteria are also used to support complex decision-making when objectives may conflict. In such cases, relevant decision factors must be identified, weighted, and balanced(Aven 2016).

Understanding an organization’s risk attitude, appetite, and tolerance is essential. Risk attitude reflects the approach to handling risk, while risk appetite refers to the amount and type of risk an organization is willing to accept. Risk tolerance defines the capacity to endure risk after mitigation efforts are in place.

Although risk criteria should be defined at the beginning of the risk assessment, they are not static and should evolve based on changing conditions, outcomes, and organizational needs.

Effective criteria development must also consider:

- Tangible and intangible risks and opportunities,
- How to define and measure consequences and likelihood (positive and negative),
- Time-related factors,
- Consistency in evaluation methods,
- The interaction and sequencing of multiple risks,
- And the organization’s overall ability to manage risk.

In sum, well-defined and regularly reviewed risk criteria are fundamental for consistent and informed risk evaluation and decision-making.

Risk tolerance reflects your ability to withstand risk exposure after implementing risk mitigation measures to achieve desired objectives and outcomes.

Although criteria for risk evaluation should be established at the outset of the risk assessment process, they are dynamic and should be subject to ongoing review and adjustment as needed.

In setting criteria for risk evaluation and decision-making support, the following factors should be considered:

- The various uncertainties, risks, and opportunities—both tangible and intangible—that may influence organizational outcomes and objectives.
- Definition and measurement of both positive and negative consequences, as well as likelihood.
- Consideration of time-related factors.
- Consistency in measurement methodologies.
- Determination of risk levels.
- Consideration of the interaction and sequencing of multiple risks.
- Organizational capacity to manage risks effectively.

These considerations are essential for developing robust risk evaluation criteria and facilitating informed decision-making processes within the organization.

Risk Assessment

Risk assessment is the overall process of:

• Risk identification - A process of finding, recognising and describing risks.

• Risk analysis - A process to comprehend the nature of risk and to determine the level of risk.

• Risk evaluation - A process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk assessment should be conducted in a systematic, iterative, and collaborative manner, drawing upon the expertise and perspectives of stakeholders. It should utilize the best available information and incorporate further investigation when necessary.

Effective communication and consultation with internal and external stakeholders are essential for the success of risk assessment activities.

Involving stakeholders in the risk assessment process serves several purposes:

- Ensuring that stakeholders' interests are thoroughly understood and considered.
- Leveraging diverse areas of expertise to identify and analyse risks effectively.
- Appropriately considering different viewpoints and concerns during risk evaluation.
- Ensuring comprehensive identification of risks, issues, and opportunities.

The risk assessment process provides decision-makers and stakeholders with insights into uncertainties, risks, and opportunities that may impact the achievement of organizational objectives, as well as the adequacy and effectiveness of existing controls.(Lazarus Alliance 2023)

The outcomes of the risk assessment serve as inputs for decision-making processes, guiding decisions on the most suitable approaches for managing risks or capitalizing on opportunities.

IEC 31010:2019 Risk management - Risk assessment techniques, an international risk assessment standard, provides further guidance on the selection and application of various techniques that can be used to help you improve the way uncertainty is taken into account and to help you understand uncertainties, risks and opportunities.

The techniques described in the standard provide a means to improve understanding of uncertainty and its implications for your decisions and actions. It can assist you in making decisions where there is uncertainty, to provide information about particular risks and as part of a process for managing risk.

Risk Assessment Techniques Outlined in ISO 31010:

Eliciting Insights from Stakeholders and Experts: This family of techniques focuses on how to gather information from SMEs and other stakeholders in an accurate and effective way. Some techniques defined here include structured brainstorming, gaining a consensus from a group of experts (the Delphi technique), distributed 1-1 brainstorming sessions (Nominal group technique), interviews, and surveys.

Identifying Risks: This family of techniques emphasizes how the organization accurately gathers information on and identifies risks within its systems. These techniques include the use of classification and taxonomies, using Failure Modes and Effects (FMEA) and Failure Modes, Effects, and Criticality (FMCEA) Analysis, using Hazard and Operability (HAZOP) studies, scenario analysis, and Structured What-If Techniques (SWiFT).

Determining Sources of Risk: This family of techniques foregrounds the capacity of an organization to properly understand the causes of risks through the study of risk relationships. These techniques include analysing intangible risk sources (Cindynic approach) and team-based causal analysis (Ishikawa analysis).

Analysing Controls: This family of techniques emphasizes the organization's ability to determine if controls are adequate and appropriate for identified risks. This includes bow-tie analysis, Hazard Analysis and Critical Control Points (HACCP), and Layers of Protection Analysis (LOPA).

Understanding Consequences: These techniques help the organization understand the more significant impact of risks depending on the context and history of the system. These techniques include Bayesian analysis, Bayesian Networks and Influence Diagrams, Business Impact Analysis (BIA), Cause-

Consequence Analysis (CCA), Event Tree Analysis (ETA), Fault Tree Analysis (FTA), Human Reliability Analysis (HRA), Markov Analysis, Monte Carlo simulation, and Privacy Impact Analysis (PIA).

Analysing Dependencies: This technique requires that the organization perform causal mapping or use chains of argument or logic showing the relationships between events, controls, and risks. This includes causal mapping and cross-impact analysis.

Providing Measure of Risk: These techniques provide ways to measure risk impact on systems or the wider public. These techniques include toxicological risk assessment, Value at Risk (VaR) assessment, and Conditional VaR.

Evaluating Significance of Risk: This family of techniques defines ways to determine how to treat risk within the organization's context. This includes testing for the principle of "reasonably practicable" for risk toleration, using Frequency-Number (F-N) diagrams and Pareto charts, assessing based on Reliability-Centered, Maintenance (RCM), and using mapping risk indices.

Selecting Between Options: These techniques relate to the organization's capability to make decisions between two more paths for risk management, including decisions regarding acceptable risk and implemented controls. These techniques will include Cost-Benefit Analysis (CBA), decision tree analysis, game theory, and Multi-Criteria Analysis (MCA).

Recording and Reporting: These techniques refer to the organization's ability to record risk information into a database to provide insights into evolving risk potential and evaluation. These techniques will include risk registers, maintaining maintenance documents, and modelling with S-curves. (Lazarus Alliance 2023)

Risk Identification

The purpose of risk identification is to find, recognise and describe risks that might help or prevent you from achieving your objectives.

The process of identifying risks allows for the explicit consideration of uncertainties. Depending on the context and scope of the assessment, all sources of uncertainty, as well as both positive and negative effects, may be pertinent.

Risk identification entails recognizing risk sources, events, their underlying causes (drivers of risk), and the potential consequences they may entail. A risk source refers to an element that possesses inherent potential to generate risk either independently or in combination with other factors.

An event, also referred to as an incident or accident, denotes a specific occurrence or alteration in a particular set of circumstances. It may encompass one or more incidents and can be triggered by various factors.

The identification process involves anticipating potential outcomes (known uncertainties) or identifying existing situations that could impact the attainment of objectives and outcomes. This encompasses recognizing risks associated with forgoing an opportunity, representing the risk inherent in taking no action and potentially missing out on opportunities for performance enhancement.

In identifying the risk, consider the following:

- What could happen - What might go wrong? What might prevent the achievement of objectives? What risks could threaten your intended outcomes?
- How could it happen - Is the risk likely to occur at all or happen again? If so, what could cause the risk event from occurring?
- . Where could it happen - Is the risk likely to occur anywhere, in any environment or place? Or is it a risk that is dependent on your location, physical area or activity?
- Why might it happen - What factors would need to be present for the risk event to occur again? Understand why a risk event might occur or be repeated.
- What might be the consequence - If the risk event were to eventuate, what consequences would, or might this have on objective and outcome? Will the consequence be felt locally, or will it impact on the whole organisation?
- Who does or can influence the outcome - How much is within your control or influence? Make sure that those with delegations, control, influence, resources and budgets are informed. This becomes more important when considering the treatments for the risk.
- Who is the risk owner - A risk owner is a person or entity with the accountability and authority to manage the risk and coordinate activities with control and treatment owners.

Relevant, appropriate and up-to-date information is important in identifying risks.

The following factors, and the relationship between these factors, should be considered during the risk identification activity:

The following factors, and the relationship between these factors, should be considered during the risk identification activity:

- tangible and intangible sources of risk;
- causes (risk drivers) and events;
- threats and opportunities;
- vulnerabilities and capabilities;
- changes in the external and internal context;
- indicators of emerging uncertainties and risks;
- the nature and value of assets and resources;
- consequences and their impact on objectives;
- limitations of knowledge and reliability of information;

- time-related factors; and
- biases, assumptions and beliefs of those involved.

Consideration should be given that there may be more than one type of outcome, which may result in a variety of tangible or intangible consequences.

Once a risk is identified, identify any existing controls such as design features, people, processes and systems.

Risk Analysis

The objective of risk analysis is to gain a comprehensive understanding of the identified risk and its attributes, encompassing, where applicable, the assessment of risk level.

Risk level, also known as risk rating, refers to the extent of a risk or combination of risks, articulated in terms of the amalgamation of consequences and their probability of occurrence.

The risk analysis process entails a thorough examination of uncertainties, sources, causative factors (drivers of risk), consequences, likelihood, events, scenarios, controls, and their efficacy. An event may have multiple underlying causes and outcomes, potentially impacting various objectives.

The extent and intricacy of risk analysis can vary based on the analysis's purpose, the accessibility and reliability of information, and the available resources.

Various analysis techniques, including qualitative, quantitative, or a blend of both, can be employed based on the specific circumstances and intended utilization.

Risk analysis should encompass the examination of factors such as:

- the probability of events and their outcomes;
- the characteristics and severity of consequences;
- intricacies and interconnections;
- temporal considerations and volatility;
- the efficacy of current mitigation measures;
- sensitivity and confidence levels.

Risk may entail diverse consequences affecting different objectives, with these consequences potentially evolving over time. For instance, the negative repercussions of a malfunction could escalate with its prolonged existence. At times, consequences stem from exposure to multiple risk sources.

The term "likelihood" can pertain to the probability of an event occurring or the likelihood of a particular outcome. It is essential to explicitly specify the parameter to which the likelihood value pertains, and to precisely define the event or consequence under consideration.

There often exist numerous interrelations and dependencies among uncertainties, risks, and opportunities. For instance, a single cause can give rise to multiple consequences, or conversely, a specific consequence may result from multiple causes.

Incorporating existing controls and evaluating their effectiveness is vital during the risk analysis process, as the level of risk is contingent upon their sufficiency and efficiency.

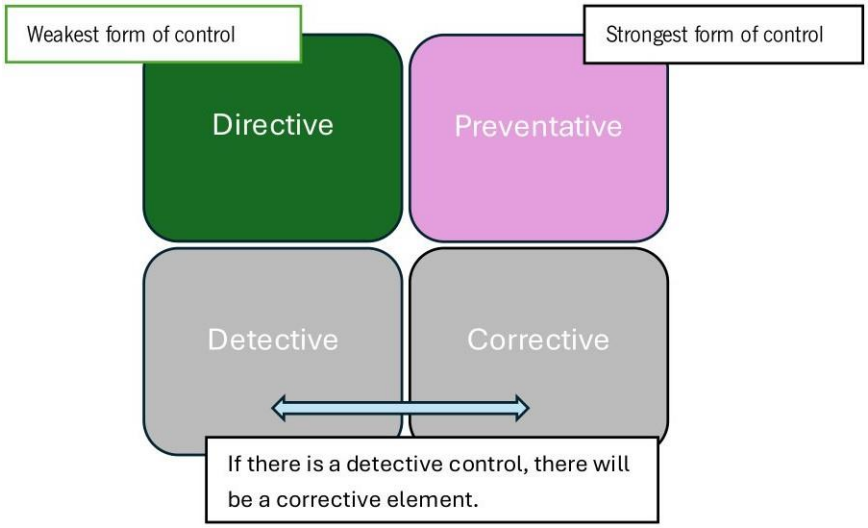


Figure 6- Risk Controls

(Institute of Risk Management (IRM) 2010)

Internal Controls

Internal controls are simply processes, policies and procedures, effected by people that ensure our internal processes, designed to modify risk, work the way we want them to so that we achieve what we want.

An organisation will have hundreds if not thousands of internal controls in place.

Preventative Controls

Preventive controls are designed to stop, discourage or pre-empt inappropriate transactions, errors or irregularities before they occur (fig. 6). These are the most desirable as they STOP problems from occurring.

Preventive controls are proactive and emphasize quality as they minimise re-work.

They tend to be more cost-effective than other controls. Preventive controls (or any control) always involve additional processes, but the processes are put up front to direct outcomes, so things won't go wrong.

Detective Controls

Detective controls (fig. 6) are designed to search for and identify errors on a timely basis after they have occurred.

Detective controls are after-the-fact controls and can also be used to measure the effectiveness of preventive controls.

In some cases, it may not be possible to have a preventative control and so detective controls are the most effective way to manage certain types of risks.

Corrective Controls

Corrective controls (fig. 6) are activated when a problem is detected, aiming to fix errors and prevent recurrence. Their effectiveness significantly impacts the overall risk level. Key factors to consider include how controls function, their status, design adequacy, potential gaps, interdependence, and any conditions that may weaken or nullify their effectiveness. Importantly, controls themselves may introduce new risks. During risk analysis, it's essential to validate assumptions about control effectiveness—especially those expected to significantly reduce risk—using insights from ongoing monitoring. Many incidents arise not from missing controls but from the failure of existing ones. Therefore, identifying and assessing current controls is vital to ensure they manage risks to an acceptable level.

The analysis process can be shaped by biases, data quality, assumptions, and methodological limitations. These influences should be documented and communicated clearly. Ultimately, the outcomes of risk analysis guide risk evaluation and help determine the appropriate treatment strategies.

Risk Evaluation

The purpose of risk evaluation is to support decisions.

Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This activity uses the understanding of risk obtained during risk analysis to make risk-informed decisions about potential future actions. Ethical, legal, financial and other considerations, including perceptions of risk, are also inputs into the decision-making process.

This can lead a decision to:

- do nothing further;
- consider risk treatment options;
- undertake further analysis to better understand the risk;
- maintain ‘existing controls;
- reconsider objectives.

The information from risk identification and analysis can be used to conclude whether the risk should be accepted and the comparative significance of the risk relative to the objectives and performance thresholds.

This provides input into decisions about whether a risk is acceptable or requires treatment and any priorities for treatment. Decisions should take account of the wider context and the actual and perceived consequences to external and internal stakeholders.

A risk may be acceptable or tolerable in the following circumstances:

- no treatment is available;
- treatment costs are prohibitive or uneconomical;
- the level of risk is low and does not warrant using resources to treat the risk;
- opportunities involved significantly outweigh the threats;
- a conscious decision has been made not to treat it.

Factors other than the magnitude of risk that can be taken into account in deciding priorities include:

- other measures associated with the risk such as the maximum or expected consequences or the effectiveness of controls:

the qualitative characteristics of events or their possible consequences;

- the views and perceptions of stakeholders;
- the cost and practicability of further treatment compared with the improvement gained; or interactions between risks including the effects of treatments on other risks.

The outcome of risk evaluation should be recorded, communicated and then validated at appropriate levels of the organisation.

Once risks have been evaluated and treatments decided, the risk assessment activity can be repeated to check that proposed treatments have not created additional adverse risks and that the risk remaining after treatment is within your risk appetite.

Risk treatment

Risk treatment involves selecting and implementing actions to modify risk, either by reducing its likelihood, its consequences, or both. This process begins after completing a risk assessment and follows an iterative cycle of choosing treatment options, executing them, evaluating their effectiveness, and determining whether the remaining risk—known as residual risk—is acceptable. If it is not, further treatment is required.

A variety of treatment options may be used, individually or in combination. These include avoiding the risk by halting the activity, reducing or increasing the likelihood to pursue opportunities, removing the risk source, altering consequences, sharing the risk with other parties (such as insurers or contractors), or

retaining the risk with full awareness. While risk sharing can help distribute potential impact, it does not remove the organization's responsibility to manage it effectively.

Choosing the most appropriate treatment requires a balance between the benefits it offers toward achieving objectives and the associated costs, effort, or trade-offs. In some cases, risk elimination might involve redesigning or scaling back a project. Where the goal is to reduce likelihood, this requires analyzing root causes and their connections to outcomes. When aiming to lessen consequences, contingency planning is essential—even when preventive controls are in place.

Stakeholder perspectives, legal obligations, and available resources must also be factored into treatment decisions. A treatment's acceptability may vary depending on how well it aligns with stakeholder values and expectations, making communication and consultation vital throughout the process.

It's important to recognize that no treatment guarantees success—some may not work as intended or may create new, unintended risks. Therefore, ongoing monitoring and review are essential to ensure treatment measures remain effective. If no viable treatment exists, the risk should still be documented and monitored regularly. Finally, decision-makers should be clearly informed about the nature and extent of any residual risks so they can decide whether further action is needed.

Preparing and implementing risk treatment plans

After selecting appropriate treatment options, organizations should develop risk treatment plans to guide implementation and monitor progress. These plans ensure that responsibilities, timelines, and resources are clearly defined and understood by all involved stakeholders.

A well-structured treatment plan should outline the rationale for chosen treatments, the expected benefits, those responsible for approval and execution, the specific actions to be taken, resources needed (including contingencies), performance indicators, assumptions, constraints, and monitoring mechanisms. The sequence and timing of actions should also be specified to ensure an effective rollout.

It's essential that treatment plans are integrated into the organization's broader management processes, and that stakeholders are consulted throughout. Once implementation begins, the effectiveness of treatments should be evaluated by asking key questions: Are the treatments achieving their intended purpose? Do they create any unintended risks (e.g., a fire sprinkler causing water damage)? Are the benefits of the treatment proportional to its cost?

Even when existing controls are deemed effective, additional treatments may still be valuable to further mitigate residual risk. After implementation, the residual risk—the level of risk remaining—should be assessed. Ideally, the residual risk will be lower than the original. However, it's important to recognize

that risks may still persist, and ongoing monitoring, documentation, and possible refinement of treatment measures are essential to ensure continuous risk control and adaptation over time.

Monitoring and review

The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes. The two key actions:

- Monitoring and identifying change from the performance level required or expected.
- Reviewing the suitability, adequacy and effectiveness of the risk management process, risk, controls and treatments to achieve established objectives. This includes determining whether the operating environment has changed and whether new risks have emerged.

Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of your risk management activities, with responsibilities clearly defined.

As part of the risk management process, risks, controls and treatments should be monitored and reviewed regularly to verify that:

- Assumptions about the uncertainties, risks and opportunities remain valid.
- Expected results and performance are being achieved
- Results of risk assessments are in line with experience or expectations.
- Risk assessment techniques are properly applied and working effectively.
- Risk treatments are effective.

Monitoring and review should take place through your risk management activities. It includes planning, gathering and analysing information, recording results and providing feedback.

The results of monitoring and review should be incorporated in your performance management, measurement and reporting activities.

Recording and reporting

The risk management activities and its outcomes should be documented and reported through appropriate mechanisms.

Recording and reporting aim to:

- communicate risk management activities and outcomes across the organisation;
- provide information for decision-making;
- improve risk management activities;
- assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

Decisions regarding the creation, retention, and management of documented information should encompass various factors, including but not restricted to their intended use, sensitivity of information, and the external and internal environment.

Reporting plays a pivotal role in organizational governance, serving to enrich the quality of communication with stakeholders and facilitating top management and oversight bodies in fulfilling their duties effectively. Factors to consider for reporting include, but are not limited to:

- differing stakeholders and their specific information needs and requirements;
- cost, frequency and timeliness of reporting;
- method of reporting; and
- relevance of the information to objectives and decision-making.
- The purpose of records is to:
- Communicate information about risk to decision-makers and other stakeholders including regulators.
- Provide a record and justification of the rationale for decisions made.
- Preserve the results of assessment for future use and reference
- Track performance and trends.
- Provide confidence that uncertainties, risks and opportunities are understood and are being managed appropriately.
- Enable verification of the assessment.
- Provide an audit trail.

3.1.2 Challenges

1. Non-Certifiable Nature: ISO 31000:2018 provides guidelines rather than prescriptive requirements and is not intended for certification purposes. This may limit its perceived authority and the external validation of an organization's risk management practices, potentially making it less compelling for stakeholders seeking assurance through certification.
2. Lack of Specificity: While ISO 31000:2018 is praised for its flexibility and broad applicability, this same generality can be a downfall in the context of IT projects with high uncertainty. The standard's lack of specificity might make it challenging for organizations to determine how to apply it effectively to complex IT projects, where specific risks and uncertainties need to be addressed with tailored strategies.
3. Implementation Challenges: Implementing ISO 31000 can be resource-intensive, requiring significant time, effort, and commitment from the organization. For IT projects that are already dealing with high uncertainty, the additional burden of implementing a comprehensive risk

management framework can be daunting and may divert resources from other critical project areas.

4. Integration with Existing Systems: While ISO 31000:2018 encourages integration with other management systems, the practicalities of aligning it with existing IT project management frameworks and methodologies can be complex. This integration challenge can hinder the seamless adoption of the standard within IT projects, potentially leading to inefficiencies or gaps in risk management practices.
5. Addressing Rapid Changes: IT projects often operate in environments characterized by rapid technological advancements and changing market conditions. The static nature of a published standard like ISO 31000:2018 may struggle to keep pace with these fast-evolving risks and uncertainties, limiting its effectiveness in providing up-to-date guidance.(Alexander S. Gillis 2023)
6. Quantitative Risk Analysis Limitations: ISO 31000:2018 primarily focuses on qualitative risk assessment and management. IT projects with high uncertainty often benefit from quantitative risk analysis methods to better understand potential impacts. The framework's lack of emphasis on quantitative methods could be a shortfall in providing the detailed risk analysis required for such projects.(Faster Capital 2024)

3.2 Risk Management in COSO ERM 2017

The figure below illustrates the Enterprise Risk Management (ERM) framework, which integrates risk management practices into an organization’s mission, strategy, and operations. It emphasizes a dynamic, iterative process where governance and culture, strategy and objective-setting, performance, and communication intersect to drive enhanced organizational value. This framework highlights how risk considerations are embedded throughout all stages—from defining mission and core values to monitoring implementation and reporting results—ensuring that risk management supports decision-making and value creation across the enterprise.



Figure 7-Process in COSO ERM 2017

3.2.1 Processes in COSO ERM 2017

Governance and Culture

Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviours, and the understanding of risk within the entity.

Governance refers to the structures, processes, and practices through which an organization's objectives are defined, implemented, and monitored. In the context of COSO ERM, effective governance is essential to ensure that risk management is integrated into the organisation's overall strategic decision-making and management processes, as shown in Figure 7.

COSO ERM emphasizes the importance of governance in providing leadership, direction, and oversight for the enterprise risk management process. This includes establishing clear roles and responsibilities for risk management at all organization levels, including the board of directors, executive management, and other key stakeholders.

Governance also involves establishing policies, procedures, and mechanisms for monitoring and reporting on risk management activities. These mechanisms help ensure accountability, transparency, and compliance with relevant regulations and standards.

Culture refers to the values, attitudes, beliefs, and behaviours that characterize an organization and its employees. A strong risk management culture is essential for embedding risk awareness and accountability throughout the organization.

COSO ERM recognizes the importance of culture in shaping how risks are perceived, assessed, and managed within an organization. A positive risk management culture encourages open communication, collaboration, and a willingness to challenge assumptions and take calculated risks.

Organizations with a strong risk management culture are more likely to proactively identify and address risks, adapt to changing circumstances, and seize opportunities for innovation and growth. COSO ERM emphasizes the need for organizations to foster a culture of risk awareness, integrity, and ethical behaviour at all levels of the organization.

Strategy and Objective-Setting

Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives translate strategy into action while serving as a basis for identifying, assessing, and responding to risk.

Alignment with Strategy: COSO ERM emphasizes the importance of aligning risk management with an organization's strategic objectives. This involves ensuring that risk management activities are integrated into strategic planning processes, so that risks and opportunities are considered when setting strategic goals.

Objective-Setting: Objectives are the goals an organization aims to achieve, and they provide a basis for identifying and assessing risks. COSO ERM encourages organizations to establish clear, measurable objectives that are aligned with their mission, vision, and values.

Risk Identification and Assessment: Once objectives are defined, COSO ERM guides organizations in identifying and assessing risks that could affect the achievement of those objectives. This involves considering both internal and external factors that may impact the organization's ability to succeed.

Risk Tolerance and Appetite: COSO ERM emphasizes the importance of understanding an organization's risk tolerance and appetite when setting objectives. Risk tolerance refers to the level of risk that an organization is willing to accept in pursuit of its objectives, while risk appetite reflects the amount of risk an organization is willing to take on to achieve its goals.

Integration with Performance Management: COSO ERM advocates integrating risk management with performance management processes. This involves monitoring and evaluating performance against objectives, while also considering the impact of risks on performance outcomes.

Continuous Improvement: Finally, COSO ERM promotes a culture of continuous improvement in strategy and objective-setting processes. This includes regularly reviewing and updating objectives considering changing internal and external factors, as well as lessons learned from past experiences.

Performance

Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks should be prioritized based on their severity and in the context of the organization’s risk

appetite. The organization then selects appropriate risk responses and adopts a portfolio view of the total risk it has assumed. The outcomes of this process must be reported to key risk stakeholders.

Objective Achievement: Within COSO ERM, performance is directly linked to the organization's ability to achieve its objectives. This includes both strategic and operational objectives, and performance is evaluated based on the extent to which these objectives are met.

Risk Management Effectiveness: COSO ERM emphasizes the importance of effective risk management as a driver of performance. Organizations are expected to implement robust risk management processes that enable them to identify, assess, and respond to efficiently and in a timely manner.

Risk Response Evaluation: Performance in COSO ERM also involves evaluating the effectiveness of the organization's risk responses. This includes assessing the adequacy of controls and mitigation strategies applied to address identified risks.

Monitoring and Reporting: COSO ERM advocates for continuous monitoring and reporting of performance related to risk management. This involves tracking key performance indicators (KPIs) and other relevant metrics to assess the effectiveness of risk management efforts and identify areas for improvement.

Integration with Decision Making: Performance in COSO ERM is closely tied to the organization's decision-making processes. Risk-informed decision making ensures that risks and opportunities are considered when making strategic and operational decisions.

Continuous Improvement: Finally, performance in COSO ERM is linked to a culture of continuous improvement. Organizations are encouraged to regularly review and enhance their risk management processes in light of changing internal and external factors, emerging risks, and lessons learned from past experiences.

Review and Revision

By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.

Periodic Review: COSO ERM emphasizes the importance of conducting periodic reviews of the organization's risk management processes. This involves assessing the effectiveness of existing risk management practices, identifying areas for improvement, and ensuring that risk management remains aligned with the organization's objectives and strategy.

Internal Control Environment: Review and revision within COSO ERM include evaluating the internal control environment to ensure that it is conducive to effective risk management. This may involve

assessing the design and operating effectiveness of internal controls and adjusting them as necessary to address any deficiencies or weaknesses.

Monitoring Activities: Review and revision also encompass ongoing monitoring activities to track the performance of risk management processes and controls. This involves regularly monitoring key risk indicators (KRIs) and other metrics to identify emerging risks and assess the effectiveness of risk responses.

External Environment Assessment: COSO ERM encourages organizations to consider changes in the external environment when conducting reviews and revisions. This includes evaluating factors such as regulatory changes, market conditions, and emerging risks that may impact the organization's risk profile and strategy.

Stakeholder Engagement: Review and revision within COSO ERM involve engaging stakeholders across the organization to gather feedback and insights on the effectiveness of risk management processes. This may include conducting surveys, interviews, or workshops to solicit input from key stakeholders.

Documentation and Revision: Finally, COSO ERM emphasizes the importance of documenting review findings and revising risk management processes accordingly. This includes updating policies, procedures, and documentation to reflect changes in the risk landscape and to ensure that risk management remains effective and relevant.

Information, Communication, and Reporting

Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

Information Management: COSO ERM stresses the importance of gathering, analysing, and managing relevant information to support the risk management process. This includes collecting data on internal and external factors that may impact the organization's objectives, as well as information related to risks and risk responses.

Risk Identification and Assessment: Information management is essential for identifying and assessing risks within the organization. This involves collecting and analysing data to understand potential threats and opportunities, as well as their potential impact on the achievement of objectives.

Decision Support: Information management also supports decision-making processes by providing decision-makers with timely and relevant data and analysis. This enables informed decision-making regarding risk responses and the allocation of resources to manage risks effectively.

Communication Channels: COSO ERM emphasizes the importance of establishing clear communication channels for sharing information related to risks and risk management activities. This includes facilitating

open communication among stakeholders at all levels of the organization, as well as with external parties such as regulators and shareholders.

Training and Awareness: Effective communication also involves providing training and raising awareness about risk management throughout the organization. This ensures that employees understand their roles and responsibilities in managing risks and are equipped with the necessary knowledge and skills to do so effectively.

Reporting Mechanisms: COSO ERM advocates for establishing robust reporting mechanisms to communicate information about risks and risk management activities to relevant stakeholders. This includes regular reporting to the board of directors, executive management, and other key stakeholders to keep them informed about the organization's risk profile and the effectiveness of risk management efforts.

Transparency and Accountability: Reporting within COSO ERM promotes transparency and accountability by providing stakeholders with accurate and timely information about the organization's risk management practices. This helps build trust and confidence among stakeholders and demonstrates the organization's commitment to managing risks effectively

3.2.2 Challenges

1. Complexity and Implementation Challenges: The COSO ERM 2017 framework's comprehensive nature can make it complex and potentially daunting for organizations to fully implement. This complexity might lead to challenges in fully integrating the framework into the unique and rapidly changing environments of IT projects, where agility and the ability to respond quickly to unforeseen changes are crucial.
2. Focus on Strategic Alignment May Overlook Technical Specificities: While the framework emphasizes strategic alignment of risk management with organizational goals, it may not sufficiently address the technical specificities and unique risks associated with IT projects. This strategic focus might result in a gap in addressing the granular, technical risks that are often prevalent in IT projects with high uncertainty (Institute of Risk Management 2017).
3. Resistance to Change: The implementation of COSO ERM 2017 requires a cultural shift towards a comprehensive view of risk management across the organization. In IT projects, where teams might be accustomed to more agile or project-specific risk management practices, there could be resistance to adopting a broader, enterprise-wide risk management approach (Committee of Sponsoring Organizations of the Treadway Commission 2017).

4. Resource Intensiveness: The successful implementation of COSO ERM 2017 can be resource-intensive, requiring significant time, effort, and commitment from across the organization. IT projects, especially those with tight deadlines and budgets, may find it challenging to allocate the necessary resources to implement the framework fully.
5. Adaptability to Rapid Technological Changes: The COSO ERM 2017 framework, while flexible, may not always be able to keep pace with the rapid technological changes and innovations characteristic of IT projects. The framework's periodic updates may not be sufficient to address the real-time, evolving risks associated with new technologies and methodologies in IT (Committee of Sponsoring Organizations of the Treadway Commission 2017).
6. Quantitative Risk Analysis Limitations: COSO ERM 2017 primarily focuses on qualitative risk assessment and management. IT projects with high uncertainty often benefit from quantitative risk analysis methods to better understand potential impacts. The framework's lack of emphasis on quantitative methods could be a shortfall in providing the detailed risk analysis required for such projects (Institute of Risk Management 2017).

3.3 Comparison between COSO ERM and ISO 31000

COSO ERM and ISO 31000 are two of the most widely used enterprise risk management (ERM) standards in the world. While both frameworks share some similarities, they also have distinct differences.

Similarities

Both standards explore risks widely. They encourage risk-taking and decision-making that is backed by risk management. They offer an approach that allows businesses to control risks so they can achieve their objectives and grow. Both COSO and ISO 31000 cover the ERM process in detail. They promote a consistent approach to the risk management process that will drive the improvement of measures and strategies.

Both frameworks are guidelines. They do not intend to enforce rules. They allow organizations to customise their approach to fit the situation of that specific business. They do not provide companies with a certification, rather, they encourage continuous improvement and better governance. Businesses that use ISO 31000 and the COSO framework can compare their own risk management policies and procedures to standards that are globally recognised.

Another similarity between the two frameworks is that they recognize the importance of being updated. They accept that we live in a fast-changing world and the risk environment does not remain the same.

Both documents get updates to add new concepts and address different kinds of situations. They provide guidelines on how to identify, assess and monitor constantly evolving risks.

Differences

1. Structure: ISO 31000 is more concise and organized, while COSO ERM is more extensive and less structured. COSO ERM is more extensive and less structured, with over 100 pages, while ISO 31000 is more concise and organized, with 16 to 32 pages.
2. Geography: ISO 31000 is the official ERM standard in over 50 countries, while COSO ERM was developed in the United States.
3. Target Audience: ISO 31000 is more generic and written for anyone interested in risk management, while COSO ERM is focused on financial reporting and auditing.
4. Framework and Process: ISO 31000 clearly separates a framework and a process, while COSO ERM combines the two concepts.
5. Risk Appetite: ISO 31000 has a brief mention of risk appetite using different terminology, while COSO ERM discusses risk appetite in great length.
6. Risk vs. Success: ISO 31000 includes avoiding negative consequences of risk and helping organizations achieve their objectives, while COSO ERM is more risk centric.
7. Customization: Both frameworks are customizable to fit an organization's specific needs and culture.
8. Implementation: ISO 31000 is designed to seamlessly integrate risk management into existing management systems, while COSO ERM promotes a consistent approach to the risk management process.
9. Updates and Improvement: Both frameworks accept that the risk environment does not remain the same and provide guidelines on how to identify, assess, and monitor constantly evolving risks.
10. Compliance Certification: Neither COSO ERM nor ISO 31000 are associated with compliance certifications, but they are guidelines that provide high-level advice and act as direction indicators for effective risk management.

The table below (table 1) illustrates the alignment between the ISO 31000:2018 risk management process and the COSO ERM 2017 components, highlighting how each step of the ISO framework maps to the corresponding ERM elements. Additionally, it outlines the organizational levels responsible for implementing these processes, ensuring a holistic integration of governance, strategy, and execution across all functions. This mapping demonstrates how the combined frameworks can provide a comprehensive and structured approach to enterprise-wide risk management.

ISO 31000:2018 Process	ERM 2017 Component	Organizational Alignment
1. Establish the Context	Risk Governance and Culture (Component 1)	Top Management
2. Risk Assessment		
└ 2.1 Risk Identification	Risk in Execution (Component 2.2)	Functional Level
└ 2.2 Risk Analysis	Risk in Execution (Component 2.2)	Functional Level
└ 2.3 Risk Evaluation	Risk in Execution (Component 2.3)	Functional Level
3. Risk Treatment	Risk Strategy / Objective Setting (Components 1 and 2.1)	Strategic Business Units (SBU)
4. Communication and Consultation	Risk Information, Communication, and Reporting (Component 4)	MIS and Risk Analysis
5. Monitoring and Review	Monitoring ERM Performance (Components 5 and 6)	Across All Processes and Departments
6. Recording and Reporting	Monitoring ERM Performance (Components 5 and 6)	Across All Processes and Departments

Table 1-Comparison between COSO ERM and ISO 31000

3.4 COSO ERM and ISO 31000:1v1 during the process

ISO 31000:2018 Process Step	Subcomponents / Detailed Activities
1. Establish the Context	Define internal and external environment, scope, and criteria
2. Risk Assessment	
└ 2.1 Risk Identification	Identify potential risk sources, events, and causes
└ 2.2 Risk Analysis	Understand risk nature, likelihood, and consequences
└ 2.3 Risk Evaluation	Compare risks against criteria to determine significance
3. Risk Treatment	Select and implement appropriate risk mitigation options
4. Communication and Consultation	Engage stakeholders continuously throughout the process
5. Monitoring and Review	Track performance of risk measures and identify emerging risks
6. Recording and Reporting	Document risk-related activities and communicate to stakeholders

Table 2-ISO 31000 Summary

The numbers used in the above-mentioned table (table 2) as to ISO 31000-2018 will be used to identify the equivalent subjects about ERM 2017 in table 3:

ERM 2017 Component	Organizational Alignment
1. Risk Governance and Culture	Top Management
2. Risk Strategy and Objective-Setting (Elements 1 and 2.1)	Strategic Business Units (SBUs)
3. Risk Execution (Elements 2.2 and 2.3)	Functional Level (Departmental and Operational Units)
4. Risk Information, Communication, and Reporting	Management Information Systems (MIS) and Risk Analysis Functions
5. Monitoring ERM Performance (Elements 5 and 6)	Organization-Wide Processes Across All Business Units and Functions

Table 3-COSO ERM 2017

1.Establishing the context for risk within an organization involves understanding various aspects that influence the scope and nature of risk analysis. This includes considering the company's environment, values, hierarchy, leadership style, and organizational objectives. In ISO standards, this context also encompasses risk strategy and objectives, which guide risk management activities(Table 2). However, in ERM 2017, risk strategy and objectives are treated as separate elements (Table 3).

In this context, risk governance serves as an overarching framework that governs the management of risk throughout the organization. It provides structure, processes, and oversight to ensure that risk management aligns with organizational objectives and is integrated into decision-making processes. Risk governance sets the tone for how risk is perceived, managed, and monitored across all levels of the organization.

Culture, on the other hand, refers to the shared values, beliefs, and behaviours that characterize an organization. It influences how risks are perceived, assessed, and managed within the company. A strong risk culture promotes transparency, accountability, and a proactive approach to risk management. This culture is often shaped by the organization's leadership and the values they espouse (Augusta De Sena and Dias n.d.).

The input of New COSO further reinforces the importance of risk governance and culture. By emphasizing the need for effective risk governance structures and fostering a risk-aware culture, organizations can enhance their ability to identify, assess, and respond to risks effectively. This approach aligns with ISO

standards by recognizing the interconnectedness of risk strategy, objectives, governance, and culture in shaping the risk landscape of an organization. Ultimately, by considering these factors holistically, organizations can establish a robust foundation for managing risk and achieving their strategic objectives.

2. In ISO 31000:2018, risk assessment encompasses the entire process of risk evaluation, including risk identification, analysis, and evaluation. This approach allows organizations to systematically assess risks by first identifying potential threats and opportunities, then analysing their causes and potential impacts, and finally evaluating their significance and likelihood. By considering these factors holistically, ISO 31000:2018 enables organizations to make informed decisions about how to manage risks effectively (Table 2).

Instead, in COSO ERM 2017, while risk identification and analysis are integral components, the term "risk assessment" is not explicitly used in the same manner as in ISO 31000:2018. Instead, risk identification is often associated with the process of objective setting, where organizations define their goals and objectives and identify potential risks that may affect their achievement. Similarly, risk analysis in COSO ERM 2017 may be referred to as assessing risks in execution, focusing on understanding the causes and potential consequences of identified risks.(Augusta De Sena and Dias n.d.).

Furthermore, in ISO 31000:2018, risk evaluation occurs after risk identification and analysis, allowing organizations to assess the significance and likelihood of identified risks. This enables organizations to prioritize risks and allocate resources effectively to manage them. In contrast, in COSO ERM 2017, while risk evaluation is essential, it may be more closely tied to the monitoring and review phase, where organizations assess the performance of their risk management efforts and measure the impact on overall company performance after implementing risk management strategies(table 3).

Overall, while both ISO 31000:2018 and COSO ERM 2017 address the concepts of risk identification, analysis, and evaluation, they may differ in terminology and timing. ISO 31000:2018 provides a structured approach to risk assessment, encompassing the entire risk management process, while COSO ERM 2017 may approach these concepts within the context of objective setting, risk in execution, and performance measurement.

3. In ISO 31000, risk treatment implies that tangible actions have been taken to address identified risks. This involves implementing specific procedures, controls, or measures aimed at mitigating, avoiding, transferring, or accepting risks to an acceptable level (table 2). These actions are typically undertaken across various stages of the risk management process, from risk identification to evaluation, treatment,

and monitoring. Thus, risk treatment in ISO 31000:2018 signifies proactive measures implemented to manage risks effectively and prevent adverse events from occurring.

Conversely, in COSO ERM, while risk treatment is an essential component, it may often be emphasized more in the monitoring phase. In this context, risk treatment involves assessing the effectiveness of previously implemented measures and adjusting them as needed. It encompasses ongoing evaluation of the performance of risk management strategies, controls, and processes to ensure they remain aligned with organizational objectives and are responsive to changing risk landscapes. Therefore, in COSO ERM, risk treatment is not solely about the initial implementation of measures but also encompasses continuous monitoring and adjustment to maintain the effectiveness of risk management efforts over time (table 3).

4. In ISO 31000:2018, "Consultation and communication" is embedded throughout each stage of the risk management process. This means that effective consultation and communication with stakeholders occur continuously, from risk identification to risk treatment and monitoring. Consultation involves seeking input and expertise from relevant parties, while communication ensures that stakeholders are informed about risks, risk management activities, and decisions made throughout the process. By integrating consultation and communication at every stage, ISO 31000:2018 promotes a collaborative and inclusive approach to risk management, enhancing the quality of risk assessments and decision-making (table 2). On the other hand, in COSO ERM 2017, consultation and communication appear more prominently toward the end of the risk management process (table 3). While consultation and communication are still essential components, they are often emphasized during the implementation and monitoring phases, following the establishment of risk management strategies and initiatives. In this context, consultation and communication serve to gather feedback on the effectiveness of risk management practices, disseminate information about risk performance, and engage stakeholders in ongoing risk management activities. While the timing may differ, the overarching goal of fostering effective consultation and communication remains consistent in both ISO 31000:2018 and COSO ERM 2017, ensuring that stakeholders are engaged and informed throughout the risk management process.

5. Monitoring and review are integral components of both the ISO 31000:2018 risk management standard and the COSO ERM 2017 framework, albeit with distinct focuses and applications. In ISO 31000:2018, monitoring and review is an interactive process that applies throughout each stage of the risk management process. This means that organizations continuously monitor and review their risk

management activities, from risk identification to risk treatment and beyond. At any given moment, organizations assess the effectiveness of their risk management efforts, gather feedback, and adjust as necessary. This iterative approach ensures that risk management remains responsive to changing circumstances and evolving risk profiles (table 2).

Alternatively, in COSO ERM 2017, monitoring and review occur after the implementation of risk management processes and serve to evaluate the performance of risk management within the company. This involves assessing whether risk management activities are effectively aligned with the organization's objectives, strategies, and governance structures (table 3). Monitoring and review in this context focus on measuring the effectiveness and efficiency of risk management practices, identifying areas for improvement, and informing decision-making processes (Augusta De Sena and Dias n.d.).

While both frameworks emphasize the importance of monitoring and review, they differ in terms of timing and focus. ISO 31000:2018 promotes a continuous, real-time approach to monitoring and review, while COSO ERM 2017 emphasizes retrospective evaluation to assess the performance of risk management processes within the organization. By incorporating elements of both frameworks, organizations can establish a robust risk management system that is both proactive and reflective, enabling them to effectively manage risks and achieve their objectives.

6. Recording and reporting are essential components of both ISO 31000:2018 and COSO ERM 2017 frameworks. ISO 31000:2018 emphasizes documenting the entire risk management process (table 2), while COSO ERM 2017 focuses on aligning risk management with organizational objectives and governance structures (table 3). Both frameworks stress the importance of transparency, accountability, and integration with governance. Effective recording and reporting facilitate transparency by providing stakeholders with clear insights into the organization's risk profile and management processes. Additionally, they support accountability by documenting roles, responsibilities, and decision-making rationale. Integrating ISO 31000:2018's documentation with COSO ERM 2017's governance framework enhances governance effectiveness and aids in achieving strategic objectives while managing uncertainty (Augusta De Sena and Dias n.d.)

4. New Approaches to Risk Management

After doing the analysis to ISO 31000:2018 and COSO ERM 2017, we can establish that there are some features that we can improve with the current technology that exist now. With that I'm going to explore these new features and using the basis of the referred frameworks upgrade the approaches to risk management in IT projects.

4.1 Digital Twins applied to Risk Management

The first feature that we are going to talk about and explain is usefulness in risk management is a new technology trend, that is Digital twins.

Digital twins in the context of risk management in IT projects refer to virtual replicas of IT systems, processes, or environments that are used to simulate, analyse, and manage risks associated with these entities(Tao et al. 2018). These digital counterparts are designed to accurately reflect their physical counterparts in real-time, using data collected from sensors and other sources. By leveraging digital twins, organizations can proactively identify, assess, and mitigate risks in IT projects without the need to interfere with the actual physical systems. This approach enables the testing of various scenarios and the evaluation of potential impacts in a controlled, virtual environment, thereby enhancing decision-making, improving safety, and optimizing system performance while minimizing the physical and financial consequences of risks.

Picking up Risk Identification and Assessment we can approach this topic in a different way using digital twins.

First in risk identification digital twins can allow for the continuous monitoring of IT systems by mirroring the real-time status of physical assets. This capability is crucial for identifying risks that could lead to system failures or performance degradation. For example, in a network infrastructure, a digital twin can monitor traffic flows, server loads, and network health, alerting IT managers to potential bottlenecks or security breaches before they escalate into more significant issues.

Second by simulating various scenarios within the digital twin environment, IT teams can predict how changes to the system might introduce new risks or exacerbate existing ones. This includes testing the impact of software updates, infrastructure changes, or the integration of new technologies. Scenario analysis helps in identifying risks associated with compatibility, performance, and security.

And finally digital twins can be programmed to recognize patterns and detect anomalies that deviate from normal operations(Grieves 2017). This is particularly useful in identifying risks such as unusual network activity that could indicate a cybersecurity threat or unexpected system behaviour that may result from a software bug or hardware malfunction.

Now related with risk assessment, digital twins are helpful for doing impact analyse because once risks are identified, digital twins can be used to assess their potential impact on the IT project. By modelling the consequences of identified risks within the virtual environment, organizations can understand the severity and reach of each risk(Project Management Institute 2017). This includes assessing the potential for data loss, service downtime, or financial implications.

It's important for risk prioritization since not all risks carry the same level of threat to an IT project. Digital twins enable IT managers to prioritize risks based on their likelihood and impact. This helps in allocating resources effectively to address the most critical risks first, ensuring that mitigation efforts are focused where they are needed most.

Digital twins facilitate the development of contingency plans by allowing teams to test various risk response strategies in a virtual setting. This can include failover testing, disaster recovery procedures, and backup systems. By evaluating different contingency plans, organizations can prepare more robust responses to potential risks(Boschert and Rosen 2016).

The insights gained from digital twins can be used to refine risk assessment models over time. As the digital twin collects more data and simulates more scenarios, it can learn to better predict and assess risks, leading to continuous improvement in risk management practices.

In the chapter of risk treatment, integrating predictive analytics with digital twins transforms risk treatment from a reactive to a proactive process. By analysing patterns and trends from historical and real-time data, digital twins can forecast potential future risks, allowing organizations to implement preventative measures before risks materialize. This predictive capability is particularly valuable in managing risks associated with IT projects, where early detection and prevention of issues can save significant time and resources.

Digital twins provide a platform for testing and validating risk treatment measures before their implementation in the physical environment. This not only ensures the effectiveness of the selected measures but also allows for their optimization. Organizations can experiment with different configurations or strategies within the digital twin to identify the most efficient and cost-effective approach to mitigating risks.

Like it was referred before digital twin give us the capacity to simulate various risk scenarios which gives us the capability to allow the exploration of different risk treatment options in a virtual setting, where the consequences of each option can be observed without any real-world repercussions. By doing so, organizations can plan and select the most effective mitigation strategies that minimize risk impact while considering cost, time, and resource constraints.

Real time monitoring in risk treatment plays again a very important role because facilitates a more dynamic and adaptive approach to it, where strategies can be adjusted in real-time based on the current state of the system. Such adaptive responses ensure that risk treatment measures remain effective under changing conditions and can prevent minor issues from escalating into significant threats (fig. 8).

Finally applying the digital twin feature will also have impact in the topic monitoring and review because it contributes to this process by providing a detailed and accurate representation of how risk management strategies have impacted the system. Through simulation and scenario analysis, digital twins can help organizations understand the consequences of their risk treatment actions, facilitating a comprehensive review of their effectiveness. This detailed feedback mechanism supports informed decision-making and the refinement of risk management practices(Boschert and Rosen 2016).

Like it was previously mentioned digital twins not only monitor and review current risk management efforts but also use predictive analytics to forecast future risks. By analysing patterns and trends in the data collected, digital twins can predict potential vulnerabilities and the likelihood of future risk events. This predictive capability enables organizations to anticipate risks before they materialize, allowing for the development of pre-emptive risk treatment strategies. As a result, the Monitoring and Review phase becomes not just a retrospective analysis but also a forward-looking process that prepares the organization for future challenges (fig. 8).

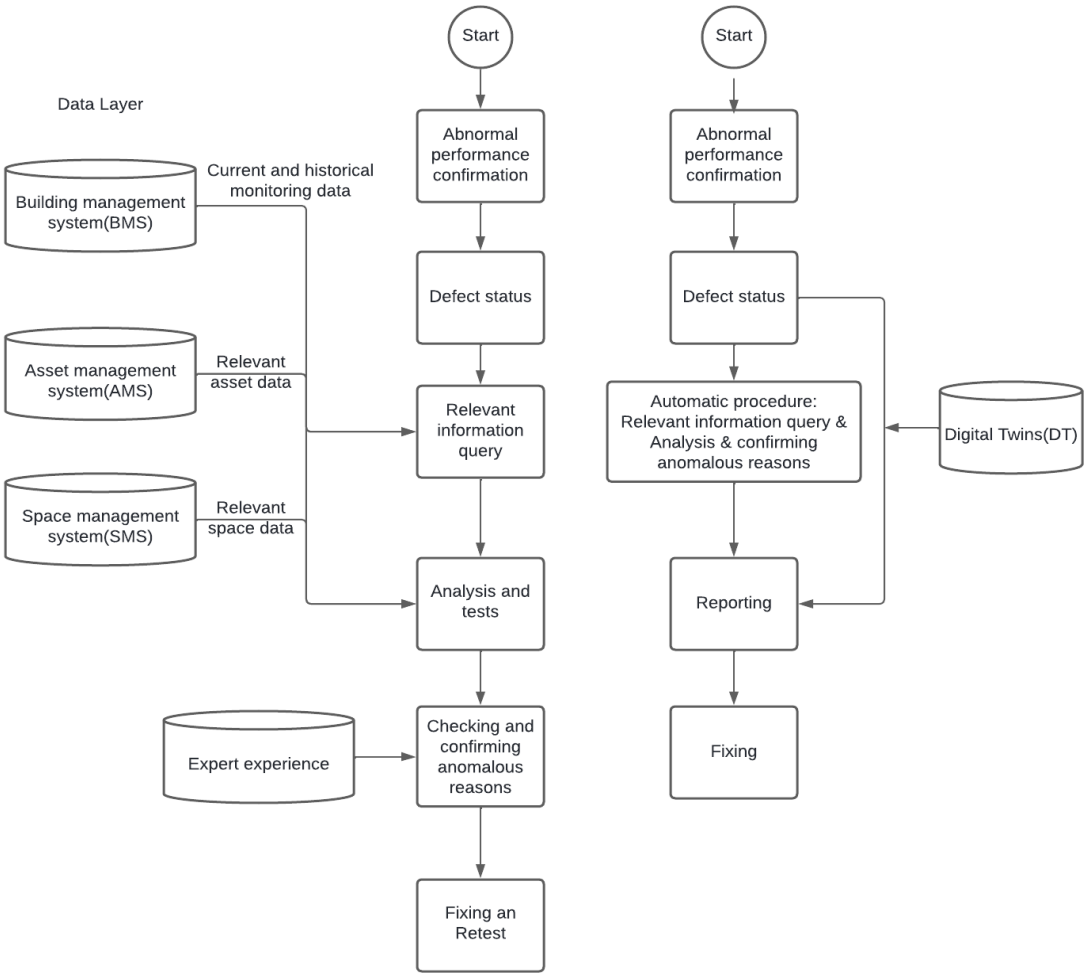


Figure 8-Traditional (Left) vs. Digital Twin-Driven Risk Management (Right)

How to apply digital twins in IT project environments:

1. Identify the risks: Organizations should identify the specific risks that can be addressed by using digital twins, such as monitoring complex systems or optimizing remote control.
2. Develop a digital twin: Organizations should develop a digital twin that accurately represents the physical system and integrates with other relevant technologies.
3. Implement the digital twin: The digital twin should be integrated into the organization's risk management processes, providing real-time data and insights to inform decision-making.
4. Monitor and adjust: Organizations should continuously monitor the performance of the digital twin and adjust their risk management strategies as needed.

By leveraging digital twins in IT project environments, organizations can improve their risk management capabilities and achieve their strategic objectives more effectively.

4.2 Artificial intelligence and Machine Learning applied to Risk Management

The second feature that we are going to discuss is Artificial Intelligence (AI).AI is becoming more well known by the days and has a lot of useful features that can be applied in risk management.

The first way that can be applied is in risk identification and assessment because it can significantly enhance the ability of organizations to identify and assess risks accurately and efficiently(Ghosh R and Sharma P 2022).

AI give us the possibility to enhanced risk identification since AI can process and analyse vast amounts of data from diverse sources at speeds and volumes far beyond human capability. This includes data from project management tools, financial systems, external databases, social media, and news feeds. By leveraging natural language processing (NLP) and other AI techniques, these systems can sift through unstructured data, identifying signals that may indicate emerging risks. For example, AI can monitor online discussions, news articles, and social media posts to detect early signs of technological trends, regulatory changes, or emerging threats that could impact an IT project. This proactive approach to risk identification allows organizations to anticipate and prepare for potential issues before they escalate(Feki MA 2020).

In relation to risk assessment AI allow us to have advanced risk assessment because once risks are identified, AI and machine learning algorithms can assess their potential impact and likelihood. This is achieved through predictive analytics, which uses historical data to identify patterns and trends that can inform future outcomes(Project Management Institute 2021). For instance, by analysing past IT project failures, AI can identify common risk factors and predict the likelihood of similar issues occurring in current projects. Machine learning models can also evaluate the interdependencies between different risks, providing a more nuanced understanding of how one risk might influence or exacerbate another. This holistic view is crucial for prioritizing risks based on their potential impact on project objectives(Project Management Institute 2021).

With the use of IA, we have the possibility to do continuous monitoring and adaptation since we can continuously monitor project parameters and external factors for new or evolving risks. This real-time risk monitoring capability ensures that risk assessments remain current and relevant, allowing for timely adjustments to risk management strategies. Moreover, AI and machine learning systems can learn from each project, improving their risk identification and assessment capabilities over time. By incorporating feedback from project outcomes and risk management actions, these systems become increasingly sophisticated and accurate in their predictions.

The second possibility that AI gives to us is to improve risk analysis and evaluation, for example AI algorithms can process historical and current project data to identify patterns that may indicate future risks. By analysing project timelines, resource allocations, budget expenditures, and other relevant data, AI can predict potential delays, cost overruns, and resource shortages. Predictive analytics can also assess the likelihood of these risks occurring, which helps project managers to prioritize which risks addressing first.

Like Digital twins Artificial Intelligence give us the possibility to simulate risk scenarios by creating models that mimic the project's environment and processes. These simulations can explore "what-if" situations, such as the impact of a key team member leaving, a critical deadline being missed, or a technology failing to perform as expected. By understanding the potential outcomes of these scenarios, project managers can develop more effective risk mitigation strategies(Gartner 2022).

AI-driven tools can rank risks based on their potential impact and likelihood, which helps project managers to allocate resources and attention efficiently. This prioritization is crucial for effective risk management, as it ensures that the most critical risks are addressed first, and resources are not wasted on low-impact or unlikely risks.

Similar to what was talked about before AI allow us to do real time monitoring which in this stage give us the capacity to do real-time monitoring of project activities, allowing for the immediate detection of deviations from the planned course. This capability is particularly valuable for identifying emerging risks quickly, enabling project managers to take corrective actions before risks escalate into more significant issues.

Finally, in what is related to risk analysis and evaluation we have the continuous learning and adaptation in which machine learning algorithms can improve their risk predictions over time by learning from new data and outcomes of past risk management actions. This continuous learning ensures that the AI models remain accurate and relevant, adapting to the changing dynamics of the project and its environment.

´The third possibility that IA gives us is the chance to give us treatment recommendations, and that works in a very specific way, which I'm going to explain next. AI can analyse vast datasets, including historical data on previous projects, to identify which risk mitigation strategies were most effective under certain conditions. By leveraging machine learning algorithms(fig. 9), AI can:

- Identify Patterns: Recognize patterns in the success or failure of past risk mitigation efforts, providing insights that might not be apparent to human analysts.
- Predict Outcomes: Predict the likely success of different risk treatment options based on the specific characteristics of the current project and its risks.

- Optimize Decisions: Recommend the most effective risk treatment strategies, optimizing for factors such as cost, time, and impact on project objectives.

For example, if an IT project faces the risk of delayed delivery due to a potential shortage of skilled developers, AI can recommend strategies such as reallocating resources from less critical tasks, hiring temporary contractors, or implementing pair programming to enhance productivity based on what has worked best in similar past scenarios.

Related to the monitoring scenario AI (fig. 9) offer us a very effective way to do it. AI can continuously monitor project parameters, external data sources, and system performance to identify new risks or changes in the status of existing risks. This involves:

- Real-Time Data Analysis: Analysing real-time data from project management tools, code repositories, and other sources to detect signs of emerging risks.
- Predictive Analytics: Using predictive analytics to forecast potential future risks based on current trends and historical data.
- Alerting Mechanisms: Automatically alerting project managers to risks that exceed predefined thresholds, enabling rapid response.

For instance, AI can monitor the progress of software development against the project timeline, using historical data to predict the likelihood of meeting milestones. If the probability of delay becomes high, the AI system can alert project managers, suggesting adjustments such as reprioritizing tasks or increasing work hours.

Finally in the chapter of communication and consultation AI-powered chatbots and virtual assistants can facilitate real-time communication and consultation among project stakeholders. They can provide stakeholders with up-to-date risk information and gather feedback to improve risk management processes.

The first feature available in this area is the real time risk communication that is made by chatbots and virtual assistants that can provide immediate, 24/7 access to risk information for project stakeholders. This is particularly valuable in dynamic project environments where risks can change rapidly, and stakeholders need to be informed about the latest developments to make timely decisions. For example, if a new risk is identified that could impact the project timeline, a chatbot can instantly notify all relevant stakeholders, ensuring that everyone is aware of the issue and can contribute to the response strategy.

The second feature is the capacity to do feedback collection and analysis since AI-powered tools can actively solicit feedback from stakeholders on risk management practices and potential risks(Project

Management Institute 2021). By engaging in dialogue with stakeholders, chatbots can gather insights and concerns that may not be captured through traditional surveys or meetings. This feedback can then be analysed using AI algorithms to identify common themes or concerns that need to be addressed, allowing project managers to refine their risk management strategies based on stakeholder input.

Chatbots can provide consistent and accurate information to all stakeholders, reducing the risk of miscommunication or misunderstanding. Since the information provided by chatbots is based on data and programmed knowledge, it eliminates the variability that can occur when information is relayed through human intermediaries. This consistency ensures that all stakeholders have the same understanding of the risks, and the risk management processes in place.

AI-powered chatbots can engage with multiple stakeholders simultaneously, making them highly scalable and efficient. This is particularly useful in large projects with many stakeholders, where individual meetings or communications would be time-consuming and impractical. Chatbots can handle routine inquiries and provide standard risk information, freeing up human project managers to focus on more complex risk management tasks.

To finalize, AI technologies can tailor communications to the specific needs and roles of different stakeholders. For instance, a chatbot can provide high-level risk summaries to executive stakeholders while offering detailed technical risk data to project team members. This level of personalization ensures that each stakeholder receives the most relevant and useful information, enhancing their ability to participate effectively in the risk management process.

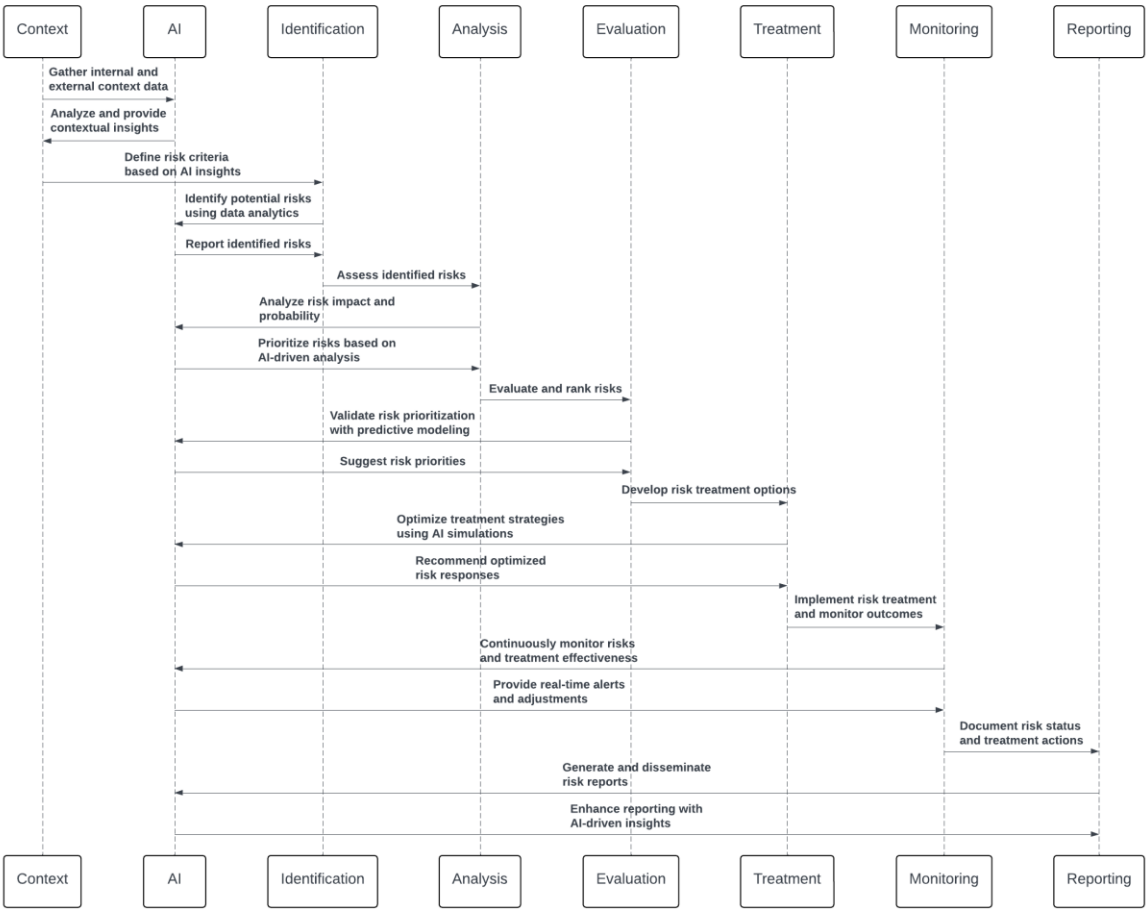


Figure 9-AI integrated in ISO 31000 2018 Process

4.3 Application of Behavioural Science in Risk Management

The next approach that we are going to talk about is different from the other two that were referred before because this one is more focused in the human factor and not so much in technology. The Application of Behavioural Science directly addresses the human factors influencing risk management practices, which are critical in IT projects characterized by high uncertainty(Hillson D and Murray-Webster R 2017). Behavioural science can help in understanding how individuals and teams perceive risk, make decisions under uncertainty, and how their behaviours can be influenced to improve risk management outcomes. This approach is particularly relevant in IT projects where rapid technological advancements and changing market conditions introduce significant uncertainties that require not only technical solutions but also an understanding of human behaviour to effectively manage risks(Hillson D and Murray-Webster R 2017).

The first way that can be applied is to enhance risk identification and assessment because the application of behavioural science can significantly improve this process by addressing cognitive biases that often

cloud judgment and decision-making(Bazerman MH and Moore DA 2013). This approach helps us mitigate biases in 5 five different ways, being them:

1. Diverse Perspectives: Encourage the inclusion of diverse viewpoints in risk assessment activities to counteract groupthink and confirmation bias. This can involve seeking input from various stakeholders, including those with differing opinions or from different organizational levels(Kutsch and Hall 2010).
2. Structured Processes: Implement structured risk identification processes, such as checklists or frameworks, that prompt consideration of a wide range of risks. This can help overcome availability bias by ensuring that less obvious but potentially significant risks are not overlooked(Bazerman MH and Moore DA 2013).
3. Challenging Assumptions: Regularly challenge existing assumptions and the status quo. This can involve revisiting and questioning the risks listed on existing risk registers to ensure they are still relevant and that new risks have not emerged(Kutsch and Hall 2010).
4. Education and Training: Provide training on cognitive biases and their effects on risk assessment. Educated team members are better equipped to recognize and counteract their own biases(Bazerman MH and Moore DA 2013).
5. Independent Reviews: Utilize independent reviews of risk assessments to provide an objective perspective that can identify biases or blind spots in the risk identification process(Sheedy E and Griffin B 2018).

We can also enhance risk assessment by leveraging Behavioural Science Techniques in which we have Behavioural Risk Assessment Models that allow us to integrate insights from behavioural science into traditional risk assessment models. This can include using decision-making experiments and simulations to study how individuals respond to various risk scenarios.

After that we have the prospect theory that when we incorporate it into risk assessments, we account for how individuals evaluate potential losses and gain differently. This can lead to a more accurate understanding of risk perceptions and tolerance levels. Finally, we have Behavioural Training and Awareness Programs that when are implemented they raise awareness about the consequences of specific behaviours and provide strategies for change. This can enhance risk literacy among employees and build a culture of risk awareness and accountability.

The second way, but in a different interval is improving risk communication, in this field the application of behavioural science allows us to understand what the audience needs, in other words it let us conduct thorough analyses to understand the needs, preferences, and communication styles of different

stakeholders. This includes identifying what information they need, how they process information, and their decision-making processes and gives us the possibility to customize communication strategies to fit the audience. For example, technical teams may require detailed data-driven reports, while executive management might prefer high-level summaries. Understanding these nuances can make communications more effective.

We can also leverage behavioural science by address cognitive biases that might affect how risks are perceived and acted upon. For instance, use framing techniques to present risk information in a way that aligns with stakeholders' attitudes and beliefs, making them more receptive to the messages and by implement nudging strategies to encourage desired behaviours without restricting freedom of choice. For example, setting defaults in decision-making processes that favour risk-aware actions can subtly influence behaviour(Project Management Institute 2021).

Finally, the application of behavioural science in the field of risk communication, will allow us to build a risk aware culture, more precisely it can encourage leaders to actively participate in risk communication, setting a tone that emphasizes the importance of risk management within the organization. Leadership endorsement can significantly enhance the credibility of the communication, and it can also help to foster an environment where stakeholders feel comfortable discussing risks openly. Promote transparency and encourage questions and discussions about risk, which can lead to more informed and engaged stakeholders(Project Management Institute 2021).

The last field that we are going to discuss the importance of the application of behavioural science is in support decision making. First, this helps to educate decision-makers about common cognitive biases that can affect judgment, such as overconfidence, anchoring, availability, and confirmation biases. Awareness can lead to more vigilant and reflective decision-making processes, and then we can implement debiasing techniques such as pre-mortem analysis, which involves envisioning a future where the project has failed and then working backward to determine what could lead to that failure. This can help in identifying potential risks that might otherwise be overlooked due to optimism bias.

Behavioural science can also facilitate group decision making by use behavioural insights to manage group dynamics during decision-making. Techniques such as the nominal group technique can help ensure that all voices are heard and that group decisions are not dominated by the loudest or most senior members(Kutsch and Hall 2010). Collaborative decision making also play a big part, more precisely by foster a collaborative decision-making environment where diverse perspectives are valued, we can encourage team members to challenge assumptions and offer alternative viewpoints, which can lead to more robust and well-rounded decisions.

Lastly, we have the possibility to enhance decision making by using heuristics evaluation, that gives us the chance to evaluate the heuristics or mental shortcuts that individuals use when making decisions under uncertainty. By understanding these heuristics, organizations can design decision-making processes that minimize their negative impact and leverage their efficiency.

And in the same field we could use judgmental bootstrapping, which involves creating statistical models that replicate human decision-making patterns. These models can then be used to support or challenge the decisions made by project managers, providing a data-driven check against subjective judgments(Bazerman MH and Moore DA 2013).

5. iRISK(Intelligent Risk Integration and Strategic Knowledge)Framework

5.1 The base of the iRISK Framework

IT projects are often characterized by high levels of complexity, uncertainty, and rapid technological evolution. Traditional risk management frameworks, such as ISO 31000 and COSO ERM, while robust, were not specifically designed to address the dynamic and fast-changing nature of IT project environments. These models typically assume a relatively stable context where risks can be identified, assessed, and mitigated in a linear and structured way.

However, modern IT projects increasingly rely on agile methodologies and continuous delivery models like DevOps, which involve iterative development cycles, frequent releases, and highly collaborative workflows. Traditional frameworks often fail to integrate seamlessly with these agile approaches, as they lack the flexibility and responsiveness required to manage risks in real time across short development sprints and rapidly evolving technical landscapes.

The iRISK framework was designed to overcome these limitations by embedding advanced tools such as Artificial Intelligence (AI) and Digital Twins, enabling real-time monitoring, predictive analytics, and dynamic scenario simulations. It also incorporates insights from behavioural science to address human factors that significantly influence risk perception and decision-making in IT teams.

Thus, a new framework tailored to IT projects is essential to ensure that risk management processes are not only proactive and dynamic but also fully compatible with agile methodologies and DevOps practices, supporting organizations in delivering value faster while effectively managing uncertainty.

In this chapter, we will combine the best features of both frameworks, as shown in Figure 7, so we can have a base for the new framework that we will discuss up front.

First, we will use governance and culture from COSO ERM:2017, because we have:

- Board Oversight and Commitment, establishing clear governance structures with board-level oversight to ensure that risk management is a strategic priority.
- Risk-Aware Culture which fosters a culture that understands and values risk management, encouraging open communication about risks at all levels of the organization.

- Ethical Standards and Integrity that promote ethical behaviour and integrity as foundational elements of the risk management process, aligning with the organization's core values and objectives.

Then we will use the principles of risk management from ISO 31000:2018 because it offers us the possibility to have:

- Integration, which ensures that risk management is integrated into all organizational processes, including decision-making and strategy formulation.
- Structured and Comprehensive, so that we can use a structured and comprehensive approach to risk management that is dynamic and responsive to the organization's needs.
- Tailored, so that we can customize the risk management practices to fit the organizational context, considering factors such as industry, culture, and regulatory environment.

The third part is the strategic objective setting from COSO ERM 2017, because it offers us the opportunity to:

- Aligning Risk Appetite and Strategy that define the organization's risk appetite and ensure it aligns with strategic objectives and operational tactics.
- Objective-Setting which set specific, measurable, achievable, relevant, and time-bound objectives that consider potential risks and opportunities.

The fourth part is the risk assessment and identification from ISO 31000:2018, which will help us in:

- Comprehensive Risk Identification, which allows us to identify risks using a variety of tools and techniques to ensure that all potential risks are considered, including those from external and internal sources.
- Risk Analysis and Evaluation, so that we can analyse and evaluate risks to determine their likelihood and impact, using qualitative and quantitative methods.

The fifth part is risk response from COSO ERM 2017, in which we will be able to:

- Selecting Risk Responses, more precisely, choose risk responses (avoid, reduce, transfer, accept) that align with the organization's risk appetite and contribute to the achievement of its objectives.
- Implementing Risk Responses, implement chosen risk responses through effective control activities and allocate resources where they are most needed.

The sixth part is performance monitoring from COSO ERM 2017, which will allow us to:

- Continuous Monitoring, in which we establish mechanisms for ongoing monitoring of risks and the effectiveness of risk responses.
- Performance Improvement, where we regularly review and revise risk management processes to improve performance and adapt to changing circumstances.

The seventh part is communication and reporting from ISO 31000:2018, which gives us the opportunity for:

- Stakeholder Engagement, which will ensure transparent and inclusive communication with all stakeholders to improve their understanding of risk management practices.
- Reporting and Documentation, which will provide regular reports on risk management activities, outcomes, and insights to support decision-making and accountability.

Finally, we have the continuous improvement, which is common to both referred frameworks, and it will enable us to:

- Learning and adapting, which promotes an environment of continuous learning and adaptation, using feedback to improve risk management practices.
- Innovation in Risk Management, which will encourage innovation in risk management techniques and tools to better address emerging risks and opportunities.

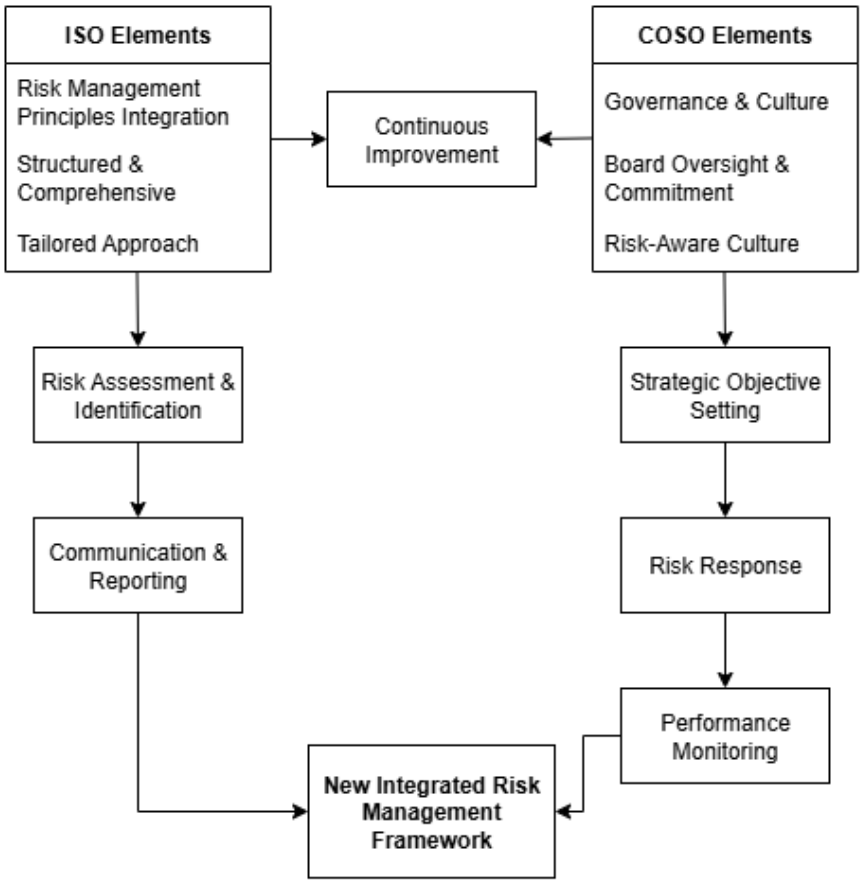


Figure 10-COSO and ISO integrated in detail

5.2 New approaches into the iRISK framework

Now we are going to put the approaches that we talked about before (chapter 4) into the framework presented in figure 10.

1.Governance and Culture

We need to ensure strong leadership and commitment to risk management that integrates technology and behavioural insights at the governance level, and we need to foster a culture that not only prioritizes risk management but also embraces technological advances such as AI and digital twins and understands human behavioural aspects that impact risk.

2. Strategic Objective-Setting

We need to set strategic objectives that leverage digital twins and AI to achieve enhanced risk monitoring and predictive capabilities, and we also need to incorporate behavioural science to ensure that strategic

objectives consider human factors and cognitive biases that may impact risk perception and decision-making.

3.Risk Assessment and Identification

In this case we will need to use digital twins to simulate different risk scenarios and their impact in a virtual environment, enabling for dynamic and real-time risk assessment.

We will also be able to implement AI algorithms to analyse large datasets for predictive insights, identify emerging risks and improve the accuracy of risk assessments.

4.Risk Response

We will use AI to help formulate and optimize risk response strategies based on predictive models and real-time data provided by digital twins.

We will also apply behavioural science principles to design risk responses that align with human behaviour and organizational culture and ensure effective implementation.

5.Performance Monitoring

We will use digital twins to continuously monitor the risk environment and the effectiveness of risk responses in real-time, and we will use AI to analyse feedback and performance data to identify trends and areas for rapid improvement.

6.Communication and Reporting

We will develop digital platforms that use digital twins and AI to visualize risks and their potential impacts, making risk communication more interactive and understandable and also craft communication strategies based on behavioural science to effectively convey risk information, ensuring it resonates with and is acted upon by all stakeholders.

7.Continuous Improvement

We will need to integrate machine learning algorithms that continuously learn from new data and experiences to improve the risk management framework over time. We will also establish feedback loops that consider behavioural responses to risk management initiatives to continually refine and adapt strategies.

To conclude this chapter, it is evident that the integration of ISO and COSO elements provides a robust foundation for enhancing risk management practices in highly uncertain IT project environments. By aligning governance, strategy, risk assessment, and continuous improvement into a coherent structure, organizations can create a dynamic and adaptive approach to managing risks effectively. As illustrated in Figure 11, the simplified framework captures the essential stages of this integrated process, ensuring a

cyclical flow that promotes learning, adaptation, and enhanced organizational resilience. This streamlined model will serve as the foundation for the new integrated risk management framework proposed in the following chapters.



Figure 11-iRISK Framework simplified

5.3 Integration and Implementation Strategy

The Integration and Implementation Strategy is a critical component of the integrated risk management framework, ensuring the successful adoption and operationalization of the combined elements so the framework can work like we expect.

So first we will begin with the phased implementation where we will have pilot projects that integrate the new technologies and behavioural science insights into the risk management process that we will evaluate the outcomes and refine the approach before a full-scale rollout (table 4). After this we will gradually expand the implementation across the organization, starting with areas that are most receptive or have the highest risk exposure. This will allow for learning and adaptation as the framework is scaled up.

Then we will go for the next part, training and development. We will develop training programmes tailored to different roles within the organization, ensuring that each team understands how to apply the new tools

and methodologies in their specific context. Then we will establish ongoing learning opportunities, such as workshops, seminars, and e-learning modules, to keep stakeholders up to date with the latest developments in risk management practices.

The next part of the integration and implementation is to engage the stakeholders in which we will involve them from all levels of the organization in the planning and development of the integrated risk management framework to ensure buy-in and address any concerns early in the process. We will also have to create channels for stakeholders to provide feedback on the framework's effectiveness and suggest improvements, this could include surveys, focus groups, and feedback sessions.

Succeeding, we have the technology and behavioural science integration, where for digital twins development we will collaborate with IT specialists to develop digital twins that accurately reflect the organization's processes and systems and to ensure that these models are accessible and provide actionable insights for risk management. For AI integration we will work with data scientists to integrate AI into the risk management process, ensuring that AI tools are aligned with the organization's data infrastructure and decision-making processes.

Relatively to behavioural science integration we will have to incorporate behavioural risk assessments into the risk identification process to understand how human factors may influence risk exposure and responses and we will design and implement programs aimed at promoting risk-aware behaviours across the organization, using behavioural science techniques such as nudging and incentives.

Finally, we will have to be monitoring and evaluating all process, and for that we will create clear performance indicators to measure the effectiveness of the integrated risk management framework. These should include both quantitative and qualitative metrics. Also, we will have to conduct regular reviews of the framework's performance, using the established indicators to assess progress and identify areas for improvement.

With all of that that was referred before we will have to be doing continuous improvement, and for that we need to ensure that the risk management framework is flexible and can be adapted as new risks emerge or as the organization's risk profile changes. Also, we will have to create an environment that encourages innovation in risk management, allowing for the testing of new ideas and technologies that could enhance the framework.

By focusing on these areas within the Integration and Implementation Strategy, organizations can effectively incorporate the strengths of our new approaches (table 4). This strategy can ensure that the framework is not only theoretically sound but also practically effective and responsive to the organization's needs.

Phase	Key Actions
Phased Implementation	- Launch pilot projects integrating new technologies and behavioural science insights. - Evaluate outcomes and refine approach before full-scale rollout. - Gradually expand to high-risk or receptive areas for learning and adaptation.
Training & Development	- Develop role-specific training programs. - Provide ongoing learning opportunities (workshops, seminars, e-learning).
Stakeholder Engagement	- Involve all levels in planning and development for buy-in. - Create feedback channels (surveys, focus groups, feedback sessions).
Technology & Behavioural Science Integration	**Digital Twins:** Work with IT specialists to ensure accurate models and actionable insights. **AI Integration:** Collaborate with data scientists to align AI with data infrastructure and decision-making. **Behavioural Science:** Incorporate behavioural risk assessments and promote risk-aware behaviours using nudging and incentives.
Monitoring & Evaluation	- Establish performance indicators (quantitative & qualitative). - Conduct regular reviews to assess progress and identify improvements.
Continuous Improvement	- Ensure flexibility to adapt to emerging risks. - Encourage innovation and testing of new ideas/technologies.

Table 4-Implementation Strategy

5.4 Benefits of the iRISK Framework

Implementing the iRISK (Intelligent Risk Integration and Strategic Knowledge) Framework (Figure 12), which synthesizes the best features of ISO 31000 and COSO while embedding advanced technologies

such as AI and digital twins, offers a range of significant benefits for organizations, particularly those managing IT projects characterized by high uncertainty.

One of the primary benefits is the enhancement of decision-making quality. By leveraging AI-driven analytics and real-time simulation capabilities provided by digital twins, the framework delivers predictive insights and dynamic data streams that significantly enrich the decision-making process. This integration not only improves the timeliness and accuracy of decisions but also helps mitigate cognitive biases, enabling more rational, objective, and evidence-based judgments. Leaders and project managers are thus better equipped to anticipate risks and seize emerging opportunities in an informed manner.

Secondly, the framework promotes a comprehensive and adaptive approach to risk identification and assessment. By unifying the strengths of ISO 31000's broad risk principles with COSO's structured risk governance, the framework ensures that a wide array of risk types—strategic, operational, technological, and external—are systematically captured and assessed. The integration of digital twin technology allows organizations to simulate diverse risk scenarios dynamically, offering continuous, real-time assessments that adapt as project environments evolve. This ongoing analysis enhances situational awareness and supports proactive risk mitigation strategies.

Another crucial benefit is the increased organizational agility and cross-functional collaboration fostered by the framework. The predictive capabilities of AI empower organizations to anticipate potential threats earlier and adapt rapidly, transforming risk management from a reactive function into a proactive, strategic capability. Additionally, the framework's structure promotes seamless collaboration across departments and management levels, dismantling organizational silos and encouraging a unified, enterprise-wide approach to risk governance. This integration enhances organizational resilience and responsiveness in volatile environments.

The framework (fig. 12) also contributes to greater cost efficiency and optimized resource allocation. By accurately forecasting risk events and their potential impacts, it reduces the frequency and severity of risk-related disruptions, leading to tangible cost savings. Furthermore, detailed insights into resource requirements provided by AI and simulation models enable organizations to allocate human, financial, and technological resources more efficiently, ensuring that investments in risk management yield maximum value.

An additional advantage is the strengthening of regulatory compliance and overall resilience. Through its structured processes aligned with recognized international standards, the framework ensures that organizations maintain compliance with relevant legal, ethical, and industry-specific requirements. By preparing for adverse scenarios and embedding resilience practices into daily operations, organizations

can maintain stability and continuity even amid significant disruptions, safeguarding their long-term viability.

Finally, the framework plays a pivotal role in enhancing stakeholder trust and organizational reputation. Effective communication strategies, informed by behavioural science principles, foster greater transparency in risk management practices, ensuring that stakeholders are well-informed and engaged. A proactive, systematic, and visibly effective approach to risk management enhances the organization's reputation as a reliable, resilient, and forward-thinking partner or service provider, thereby strengthening relationships with clients, investors, regulatory bodies, and the broader community.

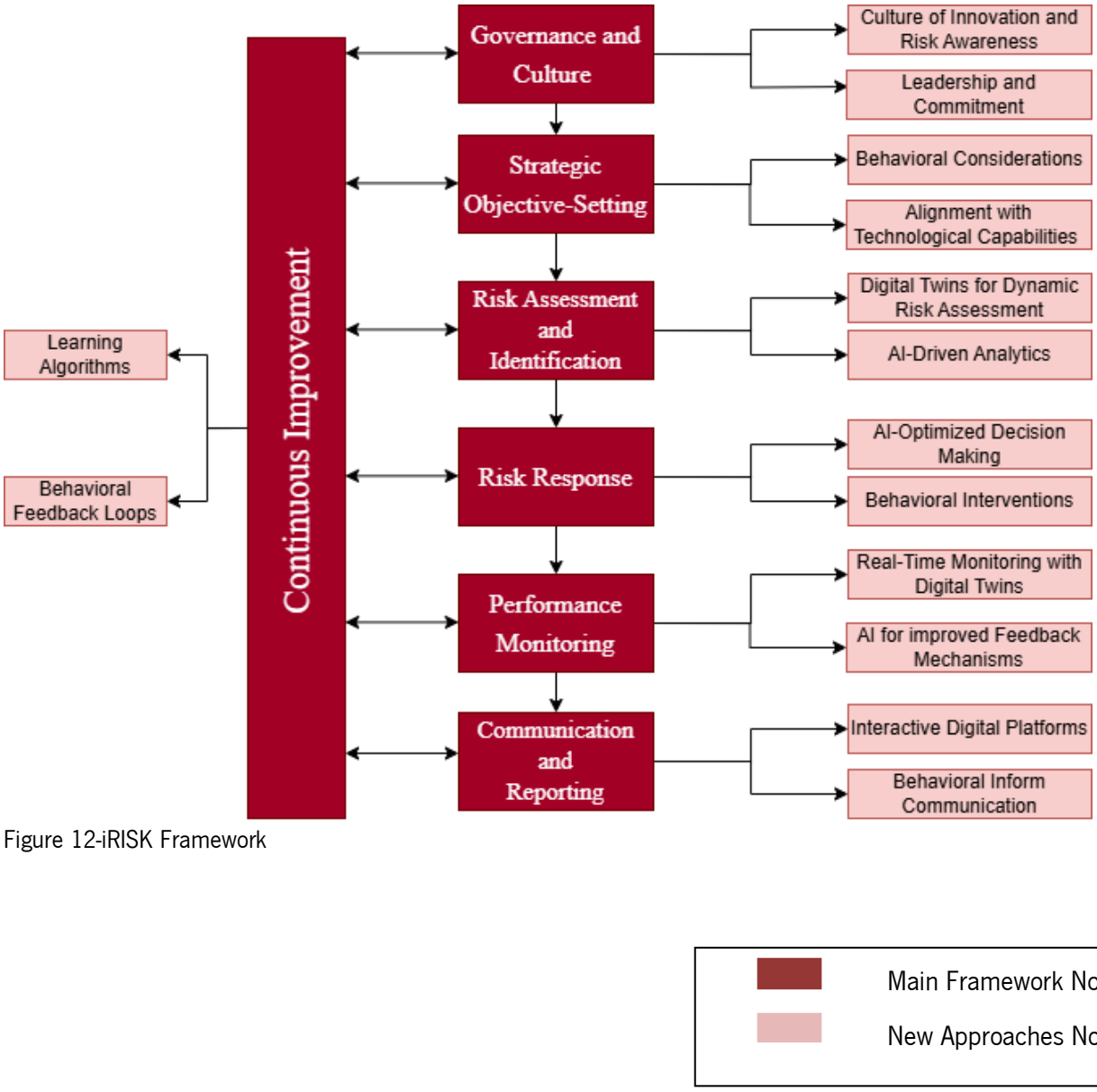


Figure 12-iRISK Framework

6. VALIDATION

Validation of the proposed framework is a crucial step to ensure its applicability, and relevance in the context under study. This chapter presents the validation process carried out through expert interviews, with the aim of assessing the strengths, limitations and potential for improvement of the framework.

To achieve this, interviews were conducted with professionals and researchers in the field, whose insights provided valuable feedback on the structure, clarity, and practical utility of the framework. The validation process follows a qualitative approach, focusing on key evaluation criteria such as applicability, completeness, and ease of implementation.

This chapter is structured as follows: first, the validation methodology is described. Next, the results of the validation process are presented, highlighting the feedback received and its implications for the refinement of the framework. Finally, there is a discussion of the strengths and areas for improvement identified, followed by concluding remarks summarizing the validation outcomes.

6.1 Evaluation Methodology

The proposed framework was validated through qualitative interviews with experts in the field. This section outlines the methodological approach used to ensure a structured and rigorous evaluation.

To validate the framework, purposive sampling was used to select participants with relevant expertise. Selection criteria included:

- Professional experience: Participants with significant practical experience in the domain related to the framework.
- Academic background: Researchers with expertise in the theoretical foundations underlying the framework.
- Familiarity with the subject: Individuals who have direct involvement with the challenges or applications addressed by the framework.

A total of 3 experts were selected to participate in the validation process.

Being these experts 1 a Business Development Manager at Whitesoft.

The second one being a Senior Manager at Deloitte Portugal.

The last one was who is a Tech Manager at Deloitte Portugal.

We are going to also use benchmarking against established frameworks such as ISO 31000 and COSO ERM to highlight advantages and limitations.

6.2 Results of Validation

A panel of industry experts and risk management professionals reviewed the framework based on usability, adaptability, and integration with existing practices. Key findings from the expert feedback include:

Strengths of the Framework

The experts highlighted several positive aspects of the thesis and the proposed framework:

- The integration of ISO31000 and COSO ERM 2017 was well received, with the expert acknowledging the effort to merge both frameworks into a new model. The comparative analysis, including the advantages and disadvantages of each framework, was particularly appreciated.
- The inclusion of digital twins, artificial intelligence (AI), and behavioral science was seen as a valuable addition. The dissertation clearly explains their relevance to risk management.
- The framework was recognized as an interesting piece of work with potential for further development beyond the scope of the thesis.

Areas for Improvement

While the expert recognized the merits of the framework, several areas for improvement were identified:

1. Lack of Visual Representation:

- The expert emphasized the need for more visual elements, such as schemas or diagrams, to enhance the comprehensibility of the framework.
- The comparison between ISO31000 and COSO ERM 2017 could benefit from more graphical illustrations to complement the text.
- A new figure should be introduced to show which components have been borrowed from ISO and COSO, providing a clear mapping between the original frameworks and the proposed model.

2. Concrete Applications for Emerging Trends:

- The experts recommended that more concrete examples of how these trends contribute to specific risk management activities should be provided in the future, including practical applications and case studies, which would enhance the credibility and usability of the framework.

6.3 Comparative Evaluation

To measure the effectiveness of the proposed framework, it was compared with ISO 31000 and COSO ERM:

Criterion	Proposed Framework	ISO 31000	COSO ERM
Adaptability	High	Moderate	Moderate
Predictive Capabilities	High	Low	Medium
Integration with Emerging Technologies	High	Low	Medium
Scalability	Moderate	High	High
Ease of Implementation	Moderate	High	Medium

Table 5-Comparative Evaluation

The comparison (table 5) shows that the proposed framework excels in terms of adaptability and predictive capabilities but requires further refinement for large-scale adoption.

6.4 Key Validation Findings

Based on the validation process, the proposed framework significantly improves the management of uncertainty in IT projects (table 5). Overall, the validation process confirmed the relevance and potential of the proposed framework as the key findings:

Effectiveness: The framework enables more accurate risk assessments and mitigation strategies, allowing for real-time adjustments in response to emerging risks. It integrates advanced analytics and AI-driven modelling to improve predictive capabilities, making risk identification more accurate and timelier.

Applicability: The framework is versatile and can be adapted to different types of IT projects, especially those with evolving requirements and high levels of uncertainty. However, improvements are needed to ensure seamless scalability in enterprise-scale projects with extensive dependencies and integrations.

Reliability: The framework consistently reduces project risk exposure by providing a structured yet flexible approach to risk management. Organizations using the framework will see improved project success rates, demonstrating that it effectively balances risk mitigation with project objectives. In addition, its structured methodologies facilitate transparency in risk reporting and decision-making.

These findings suggest that the proposed framework represents a significant advance in IT project risk management. While it outperforms traditional frameworks in terms of adaptability and predictive analysis, further refinements in scalability and implementation processes will enhance its practical applicability in diverse IT environments (table 5).

6.5 Final Evaluation and Future Perspectives

The validation process confirms that the proposed framework meaningfully advances risk management methodologies for IT projects operating in environments characterized by high uncertainty. It demonstrates the ability to deliver a more adaptive, predictive, and data-driven approach that addresses the growing complexity and dynamism of modern IT initiatives. By leveraging AI-driven analytics and digital twin technologies, the framework enables superior risk foresight, real-time scenario modelling, and proactive decision-making, allowing organizations to anticipate challenges and take pre-emptive action before risks materialize.

The integration of innovative tools and predictive models into traditional risk management processes strengthens organizational agility and responsiveness.

However, despite the evident strengths, the validation also revealed areas that require further development. Scalability remains a notable challenge, particularly when the framework is applied within large, multi-layered organizations where risk portfolios are highly complex and decentralized. Tailoring the framework's functionalities to suit diverse organizational structures without sacrificing efficiency or usability will be crucial for broader adoption. Additionally, the implementation guidelines currently provided, while practical, require further refinement and contextualization to better support organizations during the transition phase, ensuring smoother integration with pre-existing risk management practices across varying industries.

To strengthen the framework's robustness and general applicability, future research should focus on conducting large-scale real-world deployments, encompassing a variety of organizational contexts and project typologies. Longitudinal studies would also be beneficial to assess the framework's performance and adaptability over time, providing deeper insights into its long-term effectiveness, scalability, and return on investment.

Moreover, extending the framework's application beyond the IT sector—into fields such as healthcare, construction, finance, and energy—could reveal important nuances and opportunities for refinement. Such cross-industry validation would test the framework's flexibility and potentially lead to further enhancements that account for domain-specific risk characteristics.

In conclusion, while certain refinements remain necessary, the proposed framework represents a significant contribution to the advancement of risk management practices. It offers a forward-looking, technology-enabled platform that equips organizations with the strategic and operational tools required to better navigate uncertainty, mitigate risks proactively, and drive project success in an increasingly volatile and complex global environment.

7. CONCLUSION

7.1 Summary of Findings

This dissertation has explored innovative approaches to risk management in IT projects characterized by high uncertainty. Through a comprehensive analysis of existing literature, frameworks, and emerging technologies, this research has highlighted the limitations of traditional risk management methodologies in dynamic IT environments. The study examined the applicability of frameworks such as ISO 31000 and COSO ERM, alongside advanced technological interventions like Artificial Intelligence, Machine Learning, Digital Twins, and Pervasive Controls.

The research findings indicate that while traditional risk management models provide a structured approach, they often lack the flexibility required to effectively address unpredictable IT project risks. Emerging methodologies that leverage automation, real-time analytics, and behavioural sciences offer promising alternatives to enhance the adaptability, predictability, and responsiveness of risk mitigation strategies.

7.2 Contributions to Knowledge

This study contributes to the field of IT project risk management by:

- Identifying gaps in conventional risk management methodologies when applied to high uncertainty IT projects.
- Suggesting the integration of digital technologies such as AI, Behavioural Science, and Digital Twins into risk assessment and mitigation strategies.
- Demonstrating the benefits of a dynamic and iterative risk management approach over static frameworks.
- Highlighting the role of collective risk management through collaboration and information-sharing mechanisms.

These contributions provide a foundation for future research and practical applications in IT project risk management, helping organizations to navigate the complexities of rapidly evolving technology landscapes.

7.3 Practical Implications

The insights gained from this research have significant practical implications for IT project managers, risk management professionals, and organizational decision-makers. By adopting the proposed innovative risk management strategies, organizations can:

- Improve their ability to predict, assess, and respond to project risks in real-time.
- Enhance collaboration among stakeholders to foster proactive risk mitigation efforts.
- Leverage automation and data-driven decision-making to optimize project outcomes.
- Reduce the likelihood of project failure due to unanticipated uncertainties.

As organizations increasingly operate in high-uncertainty environments, incorporating flexible and technology-driven risk management approaches will become crucial for sustaining competitiveness and achieving strategic goals.

7.4 Limitations and Future Research

Despite the valuable contributions of this study, several limitations must be acknowledged. First, while this research explored emerging risk management methodologies, the implementation and real-world applicability of these approaches require further empirical validation. Additionally, the study primarily focused on IT project environments; however, the proposed methodologies could be adapted and tested across other industries facing high uncertainty.

Future research should aim to:

- Conduct case studies and pilot implementations to evaluate the effectiveness of AI-driven risk management models in IT projects.
- Investigate the ethical and regulatory challenges associated with the use of advanced analytics and automation in risk management.
- Investigate the scalability and cost-effectiveness of emerging risk management frameworks for organizations of different sizes and industries.

7.5 Final Remarks

In conclusion, the increasing complexity and unpredictability of IT projects demand a significant evolution in how risk is managed. Traditional risk management models, while still valuable, often lack the responsiveness and foresight needed to navigate rapidly changing project environments. They tend to rely heavily on reactive approaches and static planning, which may be insufficient in scenarios marked by fast-paced technological shifts, evolving stakeholder expectations, and unforeseen disruptions.

To effectively address these challenges, organizations must complement conventional frameworks with adaptive, technology-enabled strategies that are capable of continuously monitoring, analysing, and responding to emerging risks. Embracing digital transformation tools such as AI-driven analytics, real-time monitoring systems, and digital twins enables a more predictive and proactive approach to risk management—one that supports better decision-making and promotes resilience in the face of uncertainty.

This dissertation advocates for such a shift by introducing a framework that integrates modern technologies into established risk practices. The proposed approach empowers organizations not only to mitigate risks more effectively but also to identify and seize strategic opportunities that may arise from uncertainty. In doing so, it helps transform risk from a constraint into a source of competitive advantage.

Ultimately, this work represents a step toward rethinking the role of risk management in IT projects—moving from static compliance-driven processes to dynamic, intelligence-supported systems that align with the realities of today's digital landscape. By adopting such forward-looking approaches, organizations can enhance their ability to deliver successful projects, optimize resource use, and build more resilient, agile operations equipped to thrive in uncertain environments.

REFERENCES

Abrachan Pudussery. 2020. “Emerging Trends in Risk Management.”

Albinson, Nancy, Andrew Blau, and Yang Chu. n.d. *The Future of Risk: New Game, New Rules*.

Alexander S. Gillis. 2023. *ISO 31000 Risk Management*.

Alexandria Claypole. 2021. “The COSO ERM Framework Explained.”

Augusta De Sena, Alcina, and Portugal Dias. n.d. *A More Effective Audit after COSO ERM 2017 or after ISO 31000:2009?*

Aven, T. 2013. “On the Meaning of a Black Swan in a Risk Context.”

Aven, T. 2016. “Risk Assessment and Risk Management: Review of Recent Advances on Their Foundation.”

Barafort, Béatrix, Antoni-Lluís Mesquida, and Antònia Mas. 2019. “ISO 31000-Based Integrated Risk Management Process Assessment Model for IT Organizations.” *Journal of Software: Evolution and Process* 31(1):e1984. doi:https://doi.org/10.1002/smr.1984.

Barki, H. ,. Rivard, S. and Talbot, J. 2001. “‘An Integrative Contingency Model of Software Project Risk Management.’” *Journal of Management Information Systems* 17:37–69.

Bazerman MH, and Moore DA. 2013. “Judgment in Managerial Decision Making.”

Boschert, S., and R. Rosen. 2016. “The Digital Twin – Paradigm for Industry and Implications for Risk Management.”

Byron A. Love. 2017. *IT Project Management: A Geek’s Guide to Leadership. Sybex.*

Chapman, C. ,. &. Ward, S. 2011. “How to Manage Project Opportunity and Risk: Why Uncertainty Management Can Be a Much Better Approach than Risk Management.”

Christophe Veltsos. 2017. “Understanding the COSO 2017 Enterprise Risk Management Framework, Part 1: An Introduction.”

Committee of Sponsoring Organizations of the Treadway Commission. 2017. “Enterprise Risk Management – Integrating with Strategy and Performance.”

Crockford, G. Neil. 1982. “The Bibliography and History of Risk Management: Some Preliminary Observations.” *The Geneva Papers on Risk and Insurance - Issues and Practice* 7(2):169–79. doi:10.1057/gpp.1982.10.

David Cleden. 2009. *Managing Project Uncertainty*.

Debashis Saha, and Amitava Mukherjee. 2003. *Pervasive: A Paradigm for the 21st*. www.elite-care.com.

Dennis Cox. 2022. *Enterprise Risk Management in a Nutshell*.

Dionne, Georges. 2013. "Risk Management: History, Definition, and Critique." *Risk Management and Insurance Review* 16(2):147–66.

Dmitriy Stepanov. 2023. "Top 10 Best Practices to Reduce Uncertainty in Software Development."

Enterprise Risk Management Initiative Staff. 2004. "COSO's Enterprise Risk Management – Integrated Framework."

Fahad Usmani. 2024. "Risk Vs Uncertainty in Project Management."

Faster Capital. 2024. "ISO 31000: Navigating Risk Management in Uncertain Times."

G. Fernandes, S. Ward, and M. Araújo. 2013. "Identifying Useful Project Management Practices: A Mixed Methodology Approach." *International Journal of Information Systems and Project Management* 1–16.

Gartner. 2022. "Artificial Intelligence Use Cases in Risk Management." *Gartner Research*.

Gertner, Abigail, Franklin Zaromb, and Richard D. Roberts. 2016. *The Assessment of Biases in Cognition*.

Ghosh R, and Sharma P. 2022. "Artificial Intelligence in Risk Management: Applications, Challenges, and Opportunities."

Grieves, M. ,. &. Vickers. 2017. *Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems*.

H. M. Leung, V. M. Rao Tummala, and K. B. Chuah. 1998. *A Knowledge-Based System for Identifying Potential Project Risks*. Omega.

HackerOne. 2024. "What Are Bug Bounties and How Do They Work?"

Heagney, Joseph. 2022. "Fundamentals of Project Management."

Hevner, A. R., S. T. March, J. Park, and S. Ram. 2004. *Design Science in Information Systems Research.*

Hillson, D. 2009. "Managing Risk in Projects."

Hillson D, and Murray-Webster R. 2017. "Understanding and Managing Risk Attitude."

Institute of Risk Management. 2017. *From the Cube to the Rainbow Double: A Risk Practitioner's Guide to the COSO ERM Frameworks*. www.theirm.org.

Institute of Risk Management (IRM). 2010. *A Risk Practitioner's Guide to ISO 31000:2018. IRM*.

International Organization for Standardization. 2018. *ISO 31000:2018 Risk Management — Guidelines.* .

J. Tamak and D. Binda. 2013. "An Empirical Study of Risk Management & Contro." *International Journal of Advance Research in Computer Science and Software Engineering* 3–4.

Julien Haye. 2024. "Top Enterprise Risk Management Trends in 2024."

Kerzner, Harold. 2017. *Project Management: A Systems Approach to Planning, Scheduling, and Controlling*. John Wiley & Sons.

Knight, F. H. 1921. “Risk, Uncertainty, and Profit.”

Kutsch, E., and M. Hall. 2010. *Deliberate Ignorance in Project Risk Management.*

Larson, E. W. ,. &. Gray, C. F. 2011. “Project Management: The Managerial Process.”

Lazarus Alliance, Inc. 2023. “ISO 31010 and Implementing Risk Assessment Techniques.”

Lehtiranta, L. 2014. “Risk Perceptions and Approaches in Multi-Organizations: A Research Review 2000–2012.” *International Journal of Project Management*.

Megan Bell. 2022. “Risk Types in Project Management.”

Mehr, Robert, and Bob Hedges. 1963. “Risk Management in the Business Enterprise.”

Morris, P. W. G. 2013. “Reconstructing Project Management.”

Nghi M. Nguyen. n.d. “Effective Risk Management for Project Managers: A 21st Century Approach.”

Nicholas, J. M., and H. Steyn. 2020. “Project Management for Engineering, Business and Technology.”

Niehaus, Gregory, and Scott Harrington. 2003. “Risk_Management_and_Insurance.”

Olsson, R. 2007. “In Search of Opportunity Management: Is the Risk Management Process Enough?” *International Journal of Project Management*.

P. Elkington and C. Smallman. 2000. “Managing Project Risks: A Case Study from the Utilities Sector.” *International Journal of Project Management*.

Patrick, Own. 2024. “ISO 31000 Risk Management Process.”

Peixoto, Joana, Anabela Tereso, Gabriela Fernandes, and Rui Almeida. 2014. “Project Risk Management Methodology: A Case Study of an Electric Energy Organization.” *Procedia Technology* 16:1096–1105. doi:10.1016/j.protcy.2014.10.124.

Perminova, O. ,. Gustafsson, M. ,. &. Wikström, K. 2008. “Defining Uncertainty in Projects – a New Perspective.” *International Journal of Project Management*.

PMI. 2013. *A Guide to Project Management Body of Knowledge: PMBoK Guide*. Fifth Edition. USA: Project Management Institute, Inc.

Proença, Diogo, Joao Estevens, Ricardo Vieira, and José Borbinha. 2017. *Risk Management: A Maturity Model Based on ISO 31000*.

Project Management Institute. 2021. “ Next Practices: Artificial Intelligence and Project Management.”

Project Management Institute. 2017. *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*. 6th edition.

Project Management Institute. 2021. “The Human Factor in Project Management: Leveraging Behavioral Insights.”

Rick Nason. 2022. *Rethinking Risk Management*. Business Expert Press.

Riskonnect. n.d. “The Basics of ISO 31000 – Risk Management.”

RiskOptics. 2023. “The ISO 31000 Risk Management Process.”

Rouse, M. 2023. “ISO 31000 Risk Management Standard.”

Schwalbe, Kathy. 2018. “Information Technology Project Management, Loose-Leaf Version.”

Sheedy E, and Griffin B. 2018. “Risk Governance, Structures, Culture, and Behaviour: A View from the Financial Services Industry.”

Simplilearn. 2023. “13 Common Project Risks and How to Tackle Them.”

Sityata, I. ,. Botha, L., and J. Dubihlela. 2021. “Risk Management Practices by South African Universities: An Annual Report Disclosure Analysis.” *Journal of Risk and Financial Management*.

Sommerville, Ian. 2011. “Software Engineering (Ed.).” *America: Pearson Education Inc*.

Tao, F., Q. Qi, A. Liu, and A. Kusiak. 2018. “Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison.”

Team, CFI. 2021. “Uncertainty.” *The Lack of Certainty or Sureness of an Event*.

TechTarget. 2023. “What Is Risk Management and Why Is It Important?”

Troy Segal. 2023. “Operational Risk: Overview, Importance, and Examples.”

VanDerHorn, Eric, and Sankaran Mahadevan. 2021. “Digital Twin: Generalization, Characterization and Implementation.” *Decision Support Systems* 145:113524. doi:https://doi.org/10.1016/j.dss.2021.113524.

Venable, John, Jan Pries-Heje, and Richard Baskerville. 2016. “FEDS: A Framework for Evaluation in Design Science Research.” *European Journal of Information Systems* 25(1):77–89. doi:10.1057/ejis.2014.36.

VinciWorks. 2018. “How Do Biases Affect Risk Identification?”

Williams, C. A., and R. M. Heins. 1964. *Risk Management and Insurance: By C.A. Williams and R.M. Heins*. McGraw-Hill.

APPENDIX

Interview Structure

The purpose of this interview is to gather your opinion as an expert on the iRISK framework, which was developed to improve risk management in IT projects characterized by a high degree of uncertainty. Your responses will help validate the framework and, if necessary, adjust it to ensure its practical applicability.

Q1: What is your experience in risk management within IT projects?

Q2: In your perspective, what are the main limitations of traditional models (ISO 31000, COSO ERM) in highly uncertain environments?

Q3: Have you ever used or come into contact with technologies such as Artificial Intelligence (AI) or Digital Twins in the context of risk management?

Then the interviews were structured around four main components, each addressing critical dimensions of the framework:

Component 1 – Relevance and Necessity

- Q4: Do you consider that the iRISK framework addresses important gaps in traditional models such as ISO 31000 and COSO ERM? Why?
- Q5: How relevant do you consider the integration of emerging technologies, such as Artificial Intelligence and Digital Twins, for effective risk management in IT projects?

Component 2 – Clarity and Structure

- Q6: Is the iRISK framework presented in a clear and understandable manner?
- Q7: Do any aspects of the model seem overly complex or impractical for implementation?

Component 3 – Practical Applicability

- Q8: Do you believe the iRISK framework could be implemented within your organization or context?
- Q9: What challenges do you foresee in the implementation of iRISK in real-world IT project environments?

Component 4 – Validation and Improvement

- Q10: What suggestions would you make to improve the framework further?
- Q11: Which indicators do you consider essential for measuring the success of the iRISK framework implementation?

These questions provided the basis for a comprehensive evaluation of the iRISK framework from the perspective of experienced practitioners. The feedback collected was analysed and synthesized to identify strengths, limitations, and recommendations for refinement.